AN APPROACH TO ACTION FOR THE ELECTRICITY SECTOR

Working Group Forum on
Critical Infrastructure Protection

NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL
Princeton Forrestal Village
116-390 Village Boulevard
Princeton, NJ 08540-5731

Version 1.0
June 2001

Readers' Advisory

This document describes a general approach to action in many ways already implicit in the plans and programs of existing industry members to ensure reliable service. However, any institution's specific program or implementation of security considerations must reflect that organization's individual assessment of its own threats, vulnerabilities and problem consequences, as well as its local customer and community expectations, needs and tolerance for risk. Consequently, no single approach will precisely suit each organization. Therefore, this document does not represent any single or "cookbook" approach to dealing with electric sector infrastructure protection. Moreover, electric sector infrastructure protection is not a static situation. Thus this document is not intended to be, and can never be, the final product. Rather, electric sector infrastructure protection must change and evolve, just as the threats and challenges to all of the nation's critical infrastructure and the tools used to meet those threats and challenges will continue to evolve.

Whether at Pearl Harbor or at the Berlin Wall, surprise is everything involved in a government's (or in an alliance's) failure to anticipate effectively.

Thomas C. Schelling,
Forward to ***Pearl Harbor: Warning and Decision****,*
by Roberta Wohlstetter

Table of Contents

PREFACE

In May 1998, President Clinton issued Presidential Decision Directive 63 (PDD-63), Protecting America's Critical Infrastructures. The directive provides the following:

- A framework for cooperation within individual infrastructure sectors and with government for the vital mission of protecting critical infrastructure.
- Designation of "lead agencies" for each infrastructure sector.

  The U.S. Department of Energy (DOE) has been designated the lead agency for the energy industry.
- A directive for the agencies to work with their respective sectors via a "Sector Coordinator."
- A definition of Sector Coordinator functions: to assess sector vulnerabilities and develop a plan to reduce system vulnerabilities; propose a system for identifying and averting attacks; and develop a plan to alert, contain, and deflect an attack in progress and then to reconstitute minimum essential capabilities in the aftermath of an attack.

  The North American Electric Reliability Council (NERC) has been designated the Sector Coordinator for the Electricity Sector (ES).

By May 2003, remediation plans are expected to have achieved the following:

(1) to have eliminated the most significant known vulnerabilities to both physical and cyber attacks on our critical infrastructure within government agencies (such as the Power Marketing Administrations [PMA]) and key ES entities, and

(2) to have mechanisms in place for conducting ongoing periodic vulnerability assessments and remediation.

PDD-63 created the position of National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism. The Coordinator chairs the interagency Critical Infrastructure Coordinating Group. To assist the National Coordinator, the Critical Infrastructure Assurance Office (CIAO) is coordinating the drafting of a **National Plan** to determine and implement appropriate Critical Infrastructure measures. The National Plan, version 2.0, is currently in the drafting process and is the subject of ongoing interagency discussions. This "Approach to Action for the Electricity Sector" report will become part of the National Plan.

This document has two intended audiences:

- The first group includes the **Federal, State, and Local Governments, NERC, Industry of the United States, Canada, Mexico,** the **NERC Board of Trustees** (for action on those things such as an Information Sharing and Analysis Center

[ISAC] that are within the purview of NERC), and the **Department of Energy** (for which NERC has undertaken to serve as Sector Coordinator).

- The second group includes the **executive management** and the **heads of operations, physical security, and cyber security** of the approximately 3200 member organizations that comprise the ES.

The ES covers a broad range of organizations, from small power marketers with little physical infrastructure, to large transmission organizations with hundreds of substations and thousands of miles of high-voltage transmission lines. Consequently, no single approach will precisely suit each member in that broad range of institutions. Therefore, this approach to action does not reflect any single or "cookbook" approach to dealing with ES infrastructure protection.

Specific choices for action will depend on each individual institution's assessment of its needs, its risks, its infrastructure, and the potential consequences to its customers, shareholders, the communities it serves, and the continent as a whole. Inaction is inappropriate. But so is attempting to apply all of the pieces described here for every individual institution.

Just as this approach to action represents a landscape of possible actions, it is important to remember that it is also a living document. It must evolve, just as the threats and challenges to all of the nation's critical infrastructure and the tools used to meet those threats and challenges will continue to evolve. This need for change is, in fact, one of the fundamental reasons why institutions may consider and apply the concepts in this approach, and any other relevant concepts, in different ways, to differing extents, at different times.

EXECUTIVE SUMMARY

The business, technological, and national security environment in which the North American continent's electric power system infrastructure is developed, operated, and maintained is changing dramatically. New threats and vulnerabilities to the continued reliability and integrity of our infrastructure, particularly our cyber systems, are rapidly emerging. A compelling case can be made for the need to exercise due diligence in protecting and managing *both our critical physical and cyber assets.* **This approach to action documents the seriousness of the need and proposes that the North American Electric Reliability Council (NERC) and the U.S. and Canadian members of the electricity sector (ES) take an active voluntary role in the full range of Critical Infrastructure Protection (CIP) activities for the ES.**

The approach to action is organized around a four-tier model (AVOIDANCE, ASSURANCE, DETECTION, and RECOVERY) and consists of the following components:

1. **Identification of assets.** Identification of critical *physical* assets, using criteria based on national security, public health and safety, economic security, regional and national electric grid reliability, and integration of generation into the grid. Identification of critical *cyber* assets using criteria based on criticality to the reliability of the electric grid.
2. Physical and cyber security **Vulnerability Assessments (VA),** including proposed factors that need to be considered when selecting VA tools and methodologies, and a conceptual criterion by which to rate any VA methodology.
3. Physical and cyber security **Risk Assessments (RA),** including some generic threats.
4. **Mitigation plans**, acceptable risks, and risk management, considered and applied to the extent and as appropriate.
5. **Recovery and restoration,** including emergency response plans, business recovery plans, sharing utility best practices, periodic and simulation testing, and Lessons Learned reporting.
6. **Monitoring evaluation and update.** Appropriate parts of items 1 to 5 above will be revisited on a periodic basis (about every 3 to 5 years for physical security; about once a year for cyber security). However, frequency will vary, depending on the nature of the enterprise.
7. **Information sharing, education, and awareness**, including an Indications, Analysis, and Warning (IAW) program, a Standard Operating Procedure (SOP) for ES members, an Information Sharing and Analysis Center (ISAC), sharing of CIP best practices, and regional workshops on information-sharing.

8. **ES coordination**, including a national inventory of spares and the protocols to provide access to those spares in an emergency, as well as a directory of key ES contacts on the ISAC, with separate lists of contacts for the different purposes.
9. Recognition of **Interdependencies** among the Information and Communications, Fossil Fuels, Water, Law Enforcement Services, Emergency Services, Banking and Finance, Electronic Commerce, and Transportation sectors.
10. Identification of **Research and Development (R&D)** needs collected by NERC and forwarded by NERC to others, as appropriate, on a case-by-case basis.
11. Identification of **legal and regulatory issues** such as liability for failure to take action on CIP, Freedom of Information Act (FOIA) and sharing information with government, information-sharing and antitrust legislation, Federal Energy Regulatory Commission (FERC) deregulation and confidentiality, and conflicts between this program and differing local, state, regional, or federal policies and regulations that might hamper the ES CIP program.

Four areas of concern stand out—Interdependencies, (awareness of) Insider Threats, the ES-ISAC, and Cyber Security—that the ES will want to address. These areas, with opportunities and potential actions, are detailed in **Section III-D**, Conclusion.

ES customers and the general public still expect that the lights will stay on. Failure to meet this expectation will impede the progress of re-shaping the industry and will reduce customer and public confidence. Now is the time to act.

READER'S GUIDE

- **Section I** of the Report documents
  1. the need for action,
  2. the changes that drive this plan, and
  3. the interdependencies that may increase vulnerabilities but also offer opportunities for partnership.

  If you want to know more about why this Plan has been produced, and what changes in culture and technology are the driving force behind the plan, then see Section I-A and I-B. If you want to know more about the increasing opportunity and burden that interconnectedness brings, as well as its role in increasing the scope and severity of attacks, see Section I-C.

- **Section II** describes the four-tiered plan with various components of action that, taken together, represent a strong approach to Critical Infrastructure Protection. The tiers consist of the following:
  1. AVOIDANCE, including employee awareness, public awareness, and NERC outreach.
  2. ASSURANCE, including identifying critical assets, vulnerability assessments, risk assessments, mitigation plans, and periodic reassessments.
  3. DETECTION, including monitoring, reporting, and investigation.
  4. RECOVERY AND RESTORATION, including utility mutual assistance, business recovery plans, periodic and simulation testing, and Lessons Learned reporting.

  Each discussion is keyed to needs (problems), solutions (potential implementing actions), and roles and responsibilities. The section may be scanned rapidly to identify actions and responsibilities for the following:
  1. Executive Management,
  2. Heads of Operations,
  3. Heads of Cyber Security, and
  4. Heads of Physical Security.

  Suggested actions are supported by appendices with technical detail.

  If you want to know what kinds of problems are occurring now and/or are expected to occur more frequently or arise in the future; what actions and responsibilities you might have in addressing these problems; and how the overall plan might work, see Section II.

- **Section III** covers related issues that must be taken into account in implementing such an approach at the institutional and industry level, as well as working with other infrastructure industries on similar approaches. These issues include the following:

  1. Research and Development
  2. Legal and Regulatory Issues
  3. ES Coordination.

  If your interest is chiefly in the legal or regulatory aspects of this plan and of developing security issues (such as the extent of potential information sharing and the privacy and security implications); the role that science and technology can play in developing countermeasures; and the criticality of inter-utility and inter-sector linkages, see this section.

PART I: PURPOSE AND NEED

➲ *Part I provides the background and rationale to support a call for response to the Presidential Directive to take steps to counter physical and cyber threats to the electric system infrastructure by 2003.*

SECTION I-A. SCOPE AND BACKGROUND

Historical Commitment of the Industry

The North American Electric Reliability Council (NERC) has been asked on a number of occasions to serve as the electric utility industry primary point of contact for issues related to national security. Since the early 1980s, NERC has been involved with the electromagnetic pulse phenomenon, vulnerability of electric systems to state-sponsored, multi-site sabotage and terrorism, Y2k rollover impacts, and now the rapidly evolving threat of cyber intrusion. At the heart of NERC's efforts has been a commitment to work with the various federal government agencies to reduce the vulnerability of interconnected electric systems to such threats.

Federal Call to Action: PDD-63

The report of the President's Commission on Critical Infrastructure Protection (PCCIP) in October 1997 led to Presidential Decision Directive (PDD)-63, signed in May of 1998 by President Bill Clinton. In PDD-63 he stated the following:

> *The United States possesses both the world's strongest military and its largest national economy. Those two aspects of our power are mutually reinforcing and dependent. They are also increasingly reliant upon certain critical infrastructures and upon cyber-based information systems.*

Critical infrastructures are those physical- and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems, and emergency services, both governmental and private.

Historically, many of the nation's critical infrastructures have been physically and logically separate systems with little interdependence. Advances in information technology and the need to improve efficiency, however, have increasingly automated and interlinked these infrastructures. These same advances have created new vulnerabilities to equipment failures, human error, weather and other natural causes, and physical and cyber attacks. Addressing these vulnerabilities will necessarily require flexible, evolutionary approaches.

Those approaches must span both the public and private sectors, and they must protect both domestic and international security.

> *Because of our military strength, future enemies, whether nations, groups or individuals, may seek to harm us in non-traditional ways, including attacks within the United States. Our economy is increasingly reliant upon interdependent and cyber-supported infrastructures and non-traditional attacks on our infrastructure and information systems may be capable of significantly harming both our military power and our economy.*

Elsewhere in the PDD, President Clinton established "A National Goal," as follows:

> *No later than the year 2000, the United States shall have achieved an initial operating capability and no later than five years from the signing of Presidential Decision Directive 63 the United States shall have achieved and shall maintain the ability to protect our nation's critical infra- structures from intentional acts that would significantly diminish the abilities of:*
>
> - *the Federal Government to perform essential national security missions and to ensure the general public health and safety;*
> - *state and local governments to maintain order and to deliver minimum essential public services;*
> - *the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services.*
>
> *Any interruptions or manipulations of these critical functions must be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the United States.*

Role of the North American Electric Reliability Council (NERC)

The report of the PCCIP specifically commended NERC as a model for information-sharing, cooperation, and coordination between the private sector and government. PDD-63 designated the Department of Energy (DOE) as the lead Federal agency for the energy sector. In September 1998, then-Secretary of Energy Bill Richardson wrote to NERC Chairman Erle Nye seeking NERC's assistance, on behalf of the Electricity Sector (ES), in developing a program for protecting the continent's critical electricity sector infrastructure. NERC agreed to accept the role of ES Coordinator and formed a Critical Infrastructure Protection Work Group (CIPWG) under the auspices of the Operating Committee. (See also the discussion under the AVOIDANCE tier.) This document focuses on the approach that NERC and the United States, Canadian, and Mexican members of the electricity sector may take in playing an active role in the full range of critical infrastructure protection (CIP)/asset management activities.

Objective of Critical Infrastructure Protection (CIP) for the Electricity Sector (ES)

> This national initiative for the ES seeks to assure the delivery of electric power and services to its customers and to sustain public confidence in ES reliability and integrity in light of emerging physical and cyber threats to the nation's electric infrastructure and a dramatically changing political, social, economic, and technological environment.

To meet this objective, each institution that contributes to our nation's electric grid and services must understand the challenge and must work cooperatively to meet it. We are more interconnected than ever: and therefore more interdependent. The world is more technologically sophisticated. Reliable electric power helps create and sustain the nation's wealth, quality of life, and security. Both business *and* national security reasons support the need to address the changing security environment.

Intended Audiences and Participants

This document is **prepared for use** by the leadership in those electric industry institutions responsible and accountable for business, electric, security, and information technology operations.

Strategically, these include the following:

- the NERC Board of Trustees, and
- relevant agencies within the Federal government such as the Department of Energy.

Tactically, these include the following:

- utility executives/management
- heads of operations,
- heads of physical security, and
- heads of cyber security.

Framework for Action

Threat and Cooperation

Infrastructure assurance is a key element for electric entity operation: to deliver services, each entity must assure its part of the electric system every day, in planning, in operations, and in maintenance activities.

The nature and extent of the threat to reliable service, however, is new and growing. Restructured markets, application of new technologies, and the changing political and

social landscape around the world have multiplied threats and vulnerabilities—both physical and cyber, both electric and electronic.

For good business reasons, individual institutions need to respond to these threats by managing and appropriately protecting their own systems and their connections to others, to assure reliability and integrity of the national grid and to maintain public confidence. The Year 2000 migration showed how our sophisticated society's functioning depends substantially on reliable power—and how the reliability of power depends on other infrastructures. **Consequently, assessment of risk to the electric system will need to include dependencies on others, and enhanced protection will need to include cooperation with others. (**See Interdependencies, **Section I-C.)**

Implementation Principles

The electric infrastructure in North America has been tested by hurricane, earthquake, landslide, firestorm and flood, as well as by individuals who have acted with malicious intent. To cope, the sector has developed operational structures, processes, and a culture dedicated to proactive and corrective action when faced with clear and well-understood threats and consequences, especially in the physical dimension of operations.

These include NERC, backbone for action through its regional reliability councils. Policies and procedures have been established for electric control areas across the country to share information and cooperate to assure that the national electric grid remains up 24 hours a day, 365 days a year, and to minimize the potential for a disruption in one area to cascade into other areas.

Consequently, an efficient approach to action builds on these assets and follows these principles:

1. Build on or enhance existing ES structures, policies, and processes.
2. Identify and apply, to the extent and as appropriate, best practices from individual ES institutions, as well as from other industries.

This approach will go far to maintain the confidence of the industry's customers and the confidence of the general public in the reliability and integrity of this nation's electric infrastructure.

This approach to action includes a set of possible approaches to reinforcing the interconnected ES against the increasing number and varieties of threat, and thereby to protect and reinforce its individual member utilities and the vital national electric supply.

SECTION I-B. NEED FOR ACTION—WHAT HAS CHANGED?

At a time of restructuring and tight money, requests for funding for security are often met by the rhetorical management question: "Nothing has ever happened, so why spend money on security?" But in fact much has happened.

Evolving Physical Security Challenges

The state of physical security for electrical facilities varies widely, depending on local circumstances and the perceived threat. In areas with high probability of vandalism, security is fairly tight. In general, however, security at rural electrical substations consists of a fence with very minimal intrusion detection, perhaps an entry alarm at best. In fact, emphasis has generally been on protecting the public from the danger of electrocution: the fence signs might often warn of danger from high voltage, rather than against trespassing.

Much has happened in the ES—computer intrusions, sabotage, vandalism, plots to disable towers or substations; on a wider government scale, bombings that have taken military and civilian lives alike. (See **Attachments A** for the recent experiences of two fairly typical western transmission providers; **B** for a few selected incidents targeting U.S. and Canadian physical infrastructure; and **C** for a sampling of the number of people killed or injured by foreign and domestic terrorists specifically targeting U.S. citizens.)

We can learn something of the potential consequences of serious deliberate physical damage from a recent "natural" (i.e., not human-caused) event: in Auckland, New Zealand, a large underground cable serving the heart of the city failed, and businesses were left in the dark for *weeks*. The cost of replacing lost or damaged equipment and lost revenue, while very expensive, pales in comparison to the potential loss due to lawsuits.

While we may be exempt from damages as a result of terrorism, municipalities and businesses that are in financial trouble due to loss of electric service will quickly explore the issue of **whether or not we exercised due diligence in protecting critical assets**. If we fail to deal effectively with CIP, the answer will be clear that we have not.

Emerging Cyber Security Issues in the Information Age

Change is escalating in the electric industry. Industrial and commercial customers, trying to sustain competitiveness in a global market place, are pressuring suppliers of electricity to reduce prices. At the same time, the demand for and use of electricity has grown to support more sophisticated service delivery and manufacturing processes at higher speed and accuracy. U.S. electricity consumption has gone from 2.7 trillion kilowatthours in 1990 to 3.3 trillion kilowatthours in 1999 (see Table 1).

Table 1: Electric Utility Retail Sales of Electricity by Sector, 1990 through 1999 (Million Kilowatthours)

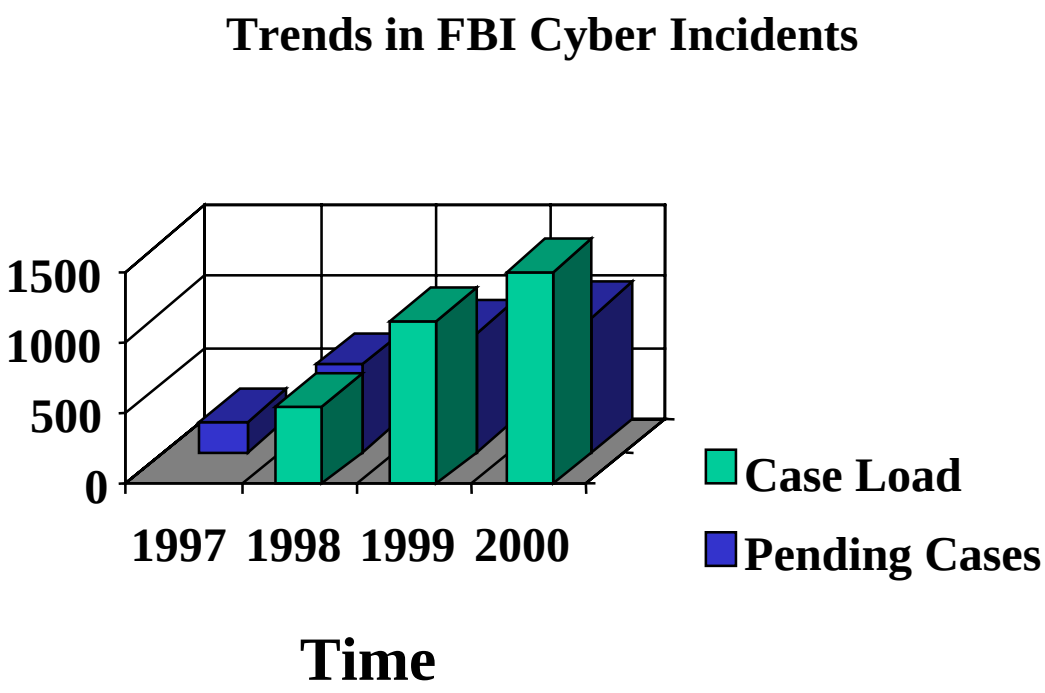
Period	Residential	Commercial	Industrial	Other	All Sectors
1990	**924,019**	**751,027**	**945,522**	**91,988**	**2,712,555**
1991	955,417	765,664	946,583	94,339	2,762,003
1992	935,939	761,271	972,714	93442	2,763,365
1993	994,781	794,573	977,164	94,944	2,861,462
1994	1,008,482	820,269	1,007,981	97,830	2,934,563
1995	1,042,501	862,685	1,012,693	95,407	3,013,287
1996	1,082,491	887,425	1,030,356	97,539	3,097,810
1997	1,075,767	928,440	1,032,653	102,901	3,139,761
1998	1,127,735	968,528	1,040,038	103,518	3,239,818
1999	**1,145,702**	**982,887**	**1,063,252**	**104,178**	**3,296,019**

Notes: Values for 1999 are preliminary. Values do not include retail sales by all energy providers (Power Marketers). Those sales are estimated to total 49 billion kilowatthours in 1999.

Sources: Energy Information Administration, Form EIA-826, "Monthly Electric Utility Sales and Revenue Report with State Distributions," and Form EIA-861, "Annual Electric Utility Report."

Restructuring, and the desire to compete efficiently and effectively in a deregulated marketplace, will continue to drive widespread, and heretofore unimagined, application of information technology to electric infrastructure operations, new types of businesses, and competition in this industry. However, accessibility to tools and techniques to do harm electronically (to disrupt or deny service, or to corrupt or destroy electronic information) has expanded dramatically. (See the figure below; also, **Attachment D** for a graphic illustration of cyber threats and actions.) Hacking has technologically become highly automated and user-friendly. Very sophisticated tools are packaged with easy-to-follow scripts. Perpetrators, who cannot be easily or quickly identified, range from the recreational hacker—who thrives on the thrill and challenge of breaking into another's computer—to the national security threat of information warriors intent on achieving strategic advantage. **Common to all threats is the well-placed insider or disgruntled employee who can bypass technological safeguards and who presents a special challenge.** (See also Insider Threat, **Section III-B)**

Figure 1: Trends in Cyber Incidents



The figure above (**Figure 1, Trends in FBI Cyber Incidents**) illustrates the growing caseload of cyber incidents being addressed by the Federal Bureau of Investigation. In many instances, access to information can determine whether an entity can successfully participate in new markets created by industry restructuring. This dependence affects operations, open market processes, emerging markets, customer relations and confidence, and corporate structure.

- **Operations**: Core operations of our electric systems depend on information technology, and that dependency is forecasted to grow. Supervisory Control and Data Acquisition (SCADA) systems are in common use to monitor, report on, and help control and regulate the flow of energy. As *The Report of the President's Commission on Critical Infrastructure Protection* noted: "These systems . . . are linked to centralized centers and corporate management systems, many of which are also connected to the outside."

- **Open Market Processes**: In the electric industry, the number of wholesale transactions has grown dramatically from 1990 to the present. These transactions are a consequence of the emerging state or regional markets resulting from deregulation, and include business conducted over the Internet, virtual private networks, and limited dedicated networks. Functions from pricing to scheduling, and metering to capacity limit notification, as well as control of generation,

transmission, and load, are being carried out over these networks. The electric business is becoming electronic commerce.

- **Emerging Markets**: The *President's Commission Report* also noted that "The movement of funds within the U.S. totally relies on computer-controlled systems and the public telecommunications networks that link them together. . . . four networks . . . transmit virtually all domestic electronic transactions, and many overseas as well." With millions of dollars worth of power traded daily over networks, failure to maintain confidentiality, integrity, or availability will not only compromise a business strategy, but will threaten the confidence of those participating in markets. Such failure can have disastrous effects, increasing market uncertainties, and potentially inspiring government intervention or regulation.

- **Customer Relations.** Many organizations have invested in highly sophisticated, information-intensive customer call centers and dispatch activities. Disruption of the underlying computer and telecommunications systems can disrupt an entity's service capability and rupture carefully nurtured customer relationships and public confidence. Consequences include regulatory scrutiny, financial penalties, and public embarrassment that can lead to loss of customer loyalty.

- **Corporate Restructuring.** As mergers, acquisitions, and partnerships (and their dissolution) become common, new partners and subsidiaries may require new links, integration, or even compartmentation of existing networks and other information assets. This may include offshore or foreign-market links. Any disruptions to information systems or corruption of its information load will have increasingly serious consequences. The benefits of using information technology come with risks that have not previously been well recognized.

In the face of these challenges, we must assure the electric industry's continued ability to deliver electric services, reliably and with integrity. This means that each ES institution must individually assure its own services, and must also work with its ES neighbors, through regional councils and through NERC, to assure regional and national capability.

Despite the rise in incidents, and the educational experience of preparing for the Year 2000 conversion exercise, surveys and anecdotal evidence have shown that **awareness of potential threats and vulnerabilities, linked to the industry's growing dependency on information systems, is relatively low.** To assure the same high levels of service capability into the 21st century, utility executives and their heads of operations, physical security, and cyber security must take steps now to protect their assets, their service, and their public image against the increasing tide of threat and disruption.

SECTION I-C. INTERDEPENDENCIES

Historically, the electric industry has been a highly regulated, "natural monopoly" industry. However, in recent years, the generation side has become less regulated and more competitive. The industry is changing from its traditional, vertically integrated structure to a deregulated structure designed to foster competition. Electricity is produced, priced, traded, and marketed differently. The industry now includes not only traditional electric utilities but also "non-utilities," including organizations that consider themselves as cogenerators, small power producers, independent power producers, and exempt wholesale generators. **None of these stands alone and independent from its competitors and cohorts**. Important dependencies include telecommunications, fossil fuels, transportation, banking and finance, electronic commerce, water, emergency services, and government services. These are outlined below; additional detail is available in **Attachment E**.

- **Fuel Dependencies.** At the end of 1998, U.S. electric generating capability totaled 775,884 megawatts (MW). Total generation increased at an annual rate of approximately 2.5 percent per year over the 1993 – 1998 period.

  Coal continues to have the largest share of total utility capacity (44%) and generation (56%) (see **Attachment E, Table E-1**). Consequently, coal transport is a sizeable dependency.

  Nuclear power represents about 14% of capacity, but about 21% of total generation.

  Petroleum and gas together account for 28% of capacity, but only 13% of generation: these sources are used more for peaking and daily cycling capacity. Natural gas, as the preferred fuel for most new generating capacity, is expected to increase its share. (Natural gas is used for 65% of nonutility generation.)

  Renewables (including hydroelectric) currently represent about 14% of capacity and about 10% of total generation.

  Balance of generation resources used is also a consideration: New York generation relies on nuclear for 27%, hydro for 23%, coal for 20%, gas for 17%, and petroleum for 12%; Hawaii relies on petroleum for 99.8% of generation. Such variations in regional structure affect the level of interdependency and the types of infrastructure assurance measures that need to be considered.

- **Interdependencies.** Infrastructure interdependency refers to the physical, electronic (cyber), and new economy (e-commerce) linkages within and among the critical national infrastructures—energy, telecommunications, banking and finance, transportation, water systems, emergency services, and government services. These linkages vary significantly in terms of scale and complexity, and typically involve a

large number of system components. These linkages must be understood in order to protect any component adequately.

Example: As noted above, the ES depends on natural gas, coal, and petroleum fuels for their generators; road and railroad transportation to get fuels (other than natural gas and some liquid petroleum products) to the generators; water for cooling and emissions reduction; and, potentially, telecommunications for monitoring system status and system control (i.e., SCADA and Energy Management Systems [EMS]).

Example: Similarly, the other critical infrastructures depend on electric power (and the other critical infrastructures) for key functions or activities. For example, natural gas depends on electric power for control systems, storage operations, and some compressor stations; water for injection purposes; and telecommunications for monitoring system status and system control (i.e., SCADA systems), as well as on road and railroad transportation, telecommunications, and petroleum fuels for repair and maintenance operations. Railroad transportation depends on electric power for signaling, crossing protection, monitoring, and certain railroad terminal operations.

- **Types of Interdependencies.** The most obvious dependencies are **physical links** (example: a substation in an electrical distribution system fails to provide electric power to a telecommunications center). Other dependencies are **linked by location and exposed environment** (example: co-location of electric power transmission lines, buried gas pipelines, and telecommunications cables that makes them more susceptible to such physical hazards as explosion, fire, flood, and seismic events, as well as sabotage). **Subtle interactions** can also occur without a direct link (example: curtailment of electricity to a natural gas pipeline compressor station could, conceivably, result in loss of natural gas to an electric generating station [or other example]). Interactions can **propagate over time**, or as a result of simultaneous failures from catastrophic or near-catastrophic **natural events** (hurricane, flood, seismic).

- **Interdependencies with Other Infrastructures.** The ES infrastructure is centrally important for operating other critical infrastructures: for example, power outages affect virtually every mode of transportation, including subways, elevators, and street traffic (no traffic lights or gasoline pumps).

  At the same time, the ES infrastructure depends strongly on the fuel delivery and storage infrastructure and on the transportation infrastructure. The ES infrastructure also depends on the telecommunications infrastructure for vital communications, and on other critical infrastructures to varying degrees for financial services and transactions, for water supply, and for emergency and government services.

A few examples of important dependencies are listed below. For every industry group, listed below, that depends on ES, there is a reciprocal dependency: ES needs those services to function in return.[1]

- *Telecommunications* are affected by extended power outages.
- *Fossil fuel systems* require electric power in virtually all aspects of the industry, including production, processing, transmission, storage, distribution, and marketing and business functions.
- *Transportation systems*—including airlines, subways, traffic control, trains, elevators, gas stations, and many others—are severely affected by electrical blackouts.
- *Banking and finance* depend on reliable electric power for operation of automatic teller machines, computers, offices, and security equipment. The financial structure (debt-equity) of the electric industry and recent innovations, such as power marketing, critically depend on the banking and finance industry.
- *Electronic commerce* depends on reliable electric power and telecommunications for operation of servers and communications equipment. Similarly, the new business and operations environments of the ES depend on the Internet and other electronic commerce systems for tags, reservations, schedules, and other information.
- *Water supply systems* depend on electricity for operations, such as pumping and metering. Water is needed for generation of electricity and is often provided by local potable water systems.
- *Emergency services* include police and fire and their communications and transport, as well as hospitals.
- *Government services* depend on reliable electricity for continuity of operations.

Actions to Address Interdependencies

The ES needs to develop a greater awareness of critical infrastructure protection issues, not only within the sector, but also more broadly, from an interdependencies perspective. If power system planners and operators fail to understand how disruptions to one infrastructure could propagate throughout the infrastructures, they will not be prepared to deal effectively with multiple infrastructure contingencies. In the highly interconnected economy of the future, hostile—and non-hostile—disruptions will have much greater ability to reverberate throughout the infrastructures, including the ES, unless "shock absorbers and circuit breakers" are built in to prevent it.

The greatest challenge is to identify and fully understand the linkages among the infrastructures (i.e., the interdependencies) and what they mean. While tools exist that allow us to model single infrastructures (such as the electric power grid), models and

[1] For detail and examples, please see Attachment D.

simulation tools for multiple, coupled infrastructures, and the requisite network databases, are rudimentary at best. Even the capability to draw general conclusions about the behaviors and properties arising from interdependent effects is very limited.

Greater awareness, coordination among the nation's infrastructure service providers and with government, and research are needed to address these issues. The research must be conducted from a holistic perspective to capture the "system-of-interacting-systems" nature of our critical infrastructures: its complex behaviors, its vulnerabilities, its robustness, and whether it degrades gracefully when stressed, the effects of its interconnections with other infrastructures, and its interfaces with human operators and users.

A possible solution would be as follows:

- Conduct regional interdependencies workshops and exercises to facilitate awareness and the development of an integrated interdependencies strategy with the following objectives:
  - Raise awareness of CIP and infrastructure interdependency issues.
  - Identify, understand, and focus attention on the important vulnerabilities associated with the ES use of other infrastructures that have a direct impact upon the ES, and develop mitigation strategies.
  - Identify ways to make infrastructure providers aware of the extent and duration of disruptions.
  - Promote a mutual understanding of infrastructure service restoration priorities, challenges, and timelines.
  - Identify and highlight roles, responsibilities, and authorities (local, county, state, and federal) for responding to and recovering from infrastructure disruptions.
  - Determine ways to foster a more effective interface among public and private sector service providers and local, county, state, and federal officials in developing and implementing critical infrastructure protection, mitigation, response, and recovery.

PART II: AN ACTION APPROACH FOR THE ELECTRIC INDUSTRY

- *Part II outlines the four-tiered security model for action to counter physical and cyber threats: AVOIDANCE, ASSURANCE, DETECTION, and RECOVERY.*
- *Part II is organized to offer a diagnosis (needs) and potential implementing actions (possible solutions) under each tier. It also offers possible guidance as to who (utility executives/ management; heads of operations; heads of physical security; heads of cyber security) might best address those possible solutions.*

A FOUR-TIERED SECURITY MODEL FOR ACTION

Assuring electric delivery and service *is* an entity's business. This four-tiered security model consists of cyber and physical security activities necessary for critical infrastructure assurance. Each tier represents a key program component. If these are completed in conjunction with the other three, the approach will help to ensure the availability and integrity of electric power systems.

Individual ES organizations already perform some limited actions to assure their part of the electric system that falls within these tiers. An effective program usually encompasses *all four* of these components, applied as individual circumstances may direct to both physical and cyber information security:

- **AVOIDANCE** Ensure electric power system integrity and availability by promoting the development and implementation of security policies, standards, and procedures; by use of outreach programs; and by providing education programs to enhance and maintain appropriate levels of cyber and physical cyber security.

- **ASSURANCE** Ensure electric power system integrity and availability by promoting the regular evaluation of physical and cyber security measures. A sub-tier component includes the identification of appropriate levels of risk management.

➲ **DETECTION**	Protect electric power systems through monitoring, identification, central reporting and analysis of operational, physical and cyber threats and/or incidents. Promote reporting of threat warnings and threat prevention information back to ES operating regions and utilities.

➲ **RECOVERY**	Promote methods for timely investigation of operational, physical or cyber security incidents and rapid recovery/restoration of services supporting the delivery of electric power services. Lessons Learned from this layer are incorporated into the other tiers.

This model is generally familiar to anyone who owns and operates part of the electric infrastructure. The tiers represent a landscape of possible action and investment, depending on:

- an organization's most important contributions to and interrelationships with the ES infrastructure,
- its balance of obligations to its customers, shareholders, and to the communities it serves, and the continent as a whole, and
- consideration of the most important information systems underlying its business and electric operations.

This model recognizes that no single approach will precisely suit each relevant institution, which may consider and apply the concepts in this model, and any other relevant concepts, in different ways, to differing extents, at different times.

SUGGESTED ROLES AND RESPONSIBILITIES

The following definitions/assignments of roles and responsibilities are suggested for this Plan.

NERC:	Serves as ES Sector Coordinator. Helps organize the industry and promotes action by its members in response to PDD-63. Promotes awareness, policies, and practices for CIP. Establishes dialogues with other critical infrastructure industries to identify interdependencies and associated risks, common concerns, and actions that could be taken. Shares good practices that might help to speed up action within its own industry and the critical infrastructure industries as a whole. Operates the ES Information Sharing and Analysis Center (ISAC). Provides sector leadership in the assurance program in general.

Utility Executives/ Management	Responsible for the development of the organization's security policy and for governance. Leads individual entity to focus on defining needs and opportunities; provides top-down emphasis and support for execution of program and individual actions, including funding, and allocation of human resources necessary to address the problem. Interacts with physical and cyber security staff to insure that the high-risk vulnerabilities that they uncover are addressed, as appropriate. Also interacts with other infrastructure management to ensure that interdependencies are addressed.
Heads of Operations:	Familiarizes self with the trends in physical and cyber security outlined in Section I-B, particularly the tables, to develop an awareness that some action is needed. (Typically ES members are [correctly] Operations-centric, and the quickest way to get something done is to gain the concern of Operations.) Helps in development of the list of critical assets. Also develops the Standing Orders (SO) or Standard Operating Procedures (SOP) to report and respond to suspected malicious events.
Heads of Physical Security	As appropriate to the nature of the entity, leads in the design and implementation of a public and employee awareness program. Where appropriate, also actively participates, or insures participation by staff, in the full range of CIP activities, from identification of critical physical assets, through vulnerability assessments, risk assessments, and mitigation plans, to recovery and restoration plans.
Heads of Cyber Security	Leads in the development or updating of the cyber security program and manual, and the development and administration of a cyber security awareness program. Actively participates in the full range of CIP activities, from identification of critical cyber assets, through scanning for vulnerabilities, tracking and installing patches, and the mitigation of those vulnerabilities that meet their cyber security risk management goals, to the development and execution of recovery and restoration plans.

SECTION II-A. AVOIDANCE

Need

➢ To protect their assets and operation, ES utilities need to be aware of, and take steps to prevent or avoid, threats to their physical and cyber plant and to those interdependencies that allow continued operation. Prevention/avoidance is the most cost-effective stage of action.

Suggested Roles

Responsible Entity	Suggested Role in Avoidance
Utility Executives/Management	▪ Policy and Governance ▪ Leadership ▪ Commitment ▪ Resources ▪ Support
Heads of Operations	▪ Heightened Awareness
Heads of Physical Security	▪ Public Awareness Program ▪ Employee Awareness Program ▪ Development of Relationship with Law Enforcement
Heads of Cyber Security	▪ Cyber Security Awareness Program ▪ Education on: Password Selection, Unauthorized Modems, Shredding of Documents, the Danger of Social Engineering, etc.

➲ *Example*: The 1999 North Valley Jewish Community Center shootings in the San Fernando Valley. Earlier, while he was casing one facility, Buford Furrow was deterred from attacking it just by being questioned about what he was doing by an alert security person. He later attacked the North Valley Jewish Community Center, wounding five people. A short time later, he shot and killed a mailman, just before being captured.

All utility employees need to be aware of the existence and scope of problems that could threaten the safe and reliable operation of their organization and of the larger ES network. Without awareness, they will fail to identify an emerging problem or to anticipate ways to counter it.

Employee awareness is the most important tool to avoid cyber security problems. Employee education is the primary means to achieve both awareness and acceptance of the problem, of opportunities to address, and of the responsibility to do so. Awareness and education also engages the recipient as a problem-solver, capturing existing knowledge, expertise, and creativity, and thus broadening and deepening the available resource.

Security (especially cyber security) intertwines technology, procedures, and culture. Organizations must work individually and together, first to identify what the problem is in terms that are relevant and appropriate to the electric system and industry as it truly operates, and as it evolves driven by market and technological forces. Consequently, outreach to raise awareness and educate electric industry leadership, operations, and security professionals is a necessary foundation for and precursor to an effective program of protection for the nation's electric infrastructure.

Policies, clear roles and responsibilities, employee understanding, attitudes, expectations and accountability for security, all that contributes to "culture," probably play the most critical part of an effective program. A comprehensive employee awareness and education program represents an organizational "best practice" and a basic component of any security program.

Public awareness is also an important tool in avoidance of physical security problems. Even in remote locations, there are often neighbors who overlook or frequently pass by electrical facilities. Handing out and posting clear and easy instructions on how to report suspicious activities, and offering a small reward, can have a significant impact on reducing theft and damage.

➲ *Example:* Bonneville Power Administration's "Crime Witness" program (imple- mented in 1994 with advertisements, postings, toll-free hotline, and rewards). From 1988 to 1994, the number of gunshot insulator units replaced averaged 1723. From1995 to 2000, the number has averaged 572. The net savings since the initiation of the program exceed $3.8M.

Key decisionmaker awareness is a central piece to the puzzle in avoiding security problems. Members of this group—focused on their markets, their customers, their obligations to the communities they serve, and their shareholders—often have many competing priorities. Security, seen as an operational responsibility, has been delegated. However, the business and operational environment is changing very rapidly, with possible consequences to which senior executives of organizations normally pay attention: operational survivability, customer relationships, new business growth, and public and shareholder confidence.

Roles

NERC Outreach

As Coordinator, NERC can promote CIP awareness, policies, and practices. It can establish dialogues with other critical infrastructure industries to identify interdependencies, associated risks, common concerns, and potential countering actions. It can share good practices to speed up action within both ES and the critical infrastructure industries as a whole.

NERC plays a critical role in disseminating information and education on electric grid reliability to all sectors and levels of the electric industry, from municipalities to rural cooperatives to generators to marketers, from Chief Executive Officers (CEOs) to electric transmission operators. It has formal and informal channels of communication of operational information and roll-out of new programs via established processes and via its member-supported working groups. NERC maintains collaborative relationships with a comprehensive group of associations that encompass nearly all of the electric industry in North America, including Canada.

NERC outreach in this arena occurs at both the strategic and tactical levels.

- Critically important is outreach to the policy and **strategic leadership** within the industry—those who are responsible for investment decisions and corporate oversight of the businesses and operations. Operations can only get so far in meeting new threats without access to needed resources and support from management.

  Key ES strategic decisionmakers must buy-in to support for CIP at the organizational, regional, and industry level. That support provides for the allocation of staff, investment, and (by policy) participation in a national initiative.

  Targeted participants include Boards of Directors or their equivalents and CEOs, as well as chief operating (COOs), financial (CFOs), information (CIOs) and security officers.

- **Tactical** outreach to operations staff is required because they have responsibility for program implementation and execution. Security, at the bottom line, is an operational responsibility.

The NERC CIPWG has already undertaken the following tasks:

- **Prepare and deliver a business case for action.** NERC and the Critical Infrastructure Assurance Office (CIAO) have developed a business case for action, couched in relevant terms. The business case is targeted specifically to CEOs, CIOs, COOs, and managers. NERC's natural channels of distribution cover almost the entire electric industry, via regional councils that manage reliability of the electric grid across the United States and Canada. NERC has affiliations with multiple associations that cover the full range of the North American electric

system ownership and operation: these councils and affiliations have agreed to participate in this outreach. Distribution of versions of this case for action has begun. This work will be continuous and will take time.

New CIP Programs are beginning to emerge from the case for action. Electric industry operations personnel already have much to do to assure reliability and the integrity of their part of the electric system. They must be convinced of the relevance of new activities to their prime mission. They must also be able to justify to their senior management the relevance of their taking on new activity. The case for action provides them with this support.

- **Develop an Action Plan for the ES.** The NERC CIPWG has developed this Approach to Action to outline the actions ES members could take in support of CIP.

- **Implement an ES-ISAC.** NERC continues development of an ES-ISAC. The ES-ISAC is expected to:

  1. Receive incident data from the ES.
  2. Assist the National Infrastructure Protection Center (NIPC) in its analysis.[2]
  3. Disseminate threat and vulnerability assessments.
  4. Carry out liaison with other ISACs.
  5. Analyze sector interdependencies.
  6. Participate in infrastructure exercises.
  7. Coordinate ES Research and Development in the CIP area.
  8. Maintain a spares database.

The Individual ES Member

NERC's overarching Sector Coordinator role is complemented by the roles and responsibilities of the various departments within a given utility. The chart at the beginning of **Section II-A** suggests where those roles and responsibilities for Avoidance might lie in response to PDD-63.

Potential Solutions/Implementing Actions

- **Training for new employees and ongoing yearly training for existing employees on physical and cyber security policies, standards and procedures.**
- **Public awareness program.**
- **Law Enforcement liaison regarding both physical and cyber security.**

[2] For more on the NIPC, please see Section II-C.

- **Programs similar to the Bonneville Power Administration's Crime Witness Program and other programs such as the Neighborhood Watch and Safe Streets Programs.**

SECTION II-B. ASSURANCE

- To protect their assets and operation, ES members need first to identify their critical assets, then conduct a vulnerability assessment of those critical assets, conduct a risk assessment of those vulnerabilities, and develop and execute mitigation plans to fix the high-risk vulnerabilities that the earlier steps have identified. Last, they need to develop a program to reassess the state of their security periodically.

Suggested Roles

Responsible Entity	Suggested Role in Assurance
Utility Executives/Management	▪ Policy and Governance ▪ Leadership ▪ Commitment ▪ Resources ▪ Support
Heads of Operations	▪ Lead or Assist in Identification of Critical Assets ▪ Host Vulnerability Assessments ▪ Participate in Interdependency Workshops ▪ Provide Operational Expertise to Vulnerability Assessments and Risk Assessments ▪ Help Evaluate Mitigation Options
Heads of Physical Security	▪ Lead or Assist in Identification of Critical Physical Assets ▪ Lead Physical Security Vulnerability Assessment and Risk Assessment Team ▪ Participate in Interdependency Workshops ▪ Lead or Assist with Physical Security Mitigation
Heads of Cyber Security	▪ Lead or Assist in Identification of Critical Cyber Assets ▪ Lead Cyber Security Vulnerability Assessment, Risk Assessment, and Mitigation Team ▪ Participate in Interdependency Workshops

Need/Discussion

Physical and Cyber security risks are typically managed very differently (see **Attachment F** for more information on risk management). There are good reasons for this difference. The cyber threat is evolving so rapidly that an organization must respond very quickly. By contrast, the physical threat is evolving more slowly and the state-of-art in physical security is a more deliberate approach, where many solutions are expensive and take a comparatively great deal of time to apply. However, they have several problems in common at the ASSURANCE tier:

1. Most organizations have no holistic risk management process (a problem beyond the scope of this document).
2. Most organizations have cyber security and physical security separated organizationally. Some even have general Information Technology (IT) and EMS security separate. This makes communication and cooperation more difficult.
3. Most organizations do not approach risk management, even within the silos, in an organized way through use of a rigorous risk management process.
4. Most siloed organizations are, in general, unaware of visualization tools such as Risk Management Maps, Risk Decision Support Diagrams, etc., which could help them balance risk management decisions across the whole organization.

Potential Solutions/ Implementing Actions

Some ES members could benefit by establishing the organization's policy for things such as how they will react to security events, how they will conduct internal communications during those events, and who will have the ability to contact law enforcement and other external entities.

There are five primary steps to increasing assurance.

1. **Identify critical assets.**
2. **Conduct Vulnerability Assessments of those critical assets.**
3. **Conduct Risk Assessments of those vulnerabilities.**
4. **Develop and implement mitigation plans.**
5. **Develop a program to reassess the state of their security periodically.**

Each of these is discussed below.

Identification of Critical Assets

In order to protect assets effectively and efficiently, the ES utility must first identify which assets are critical.

Critical **physical** assets for the electric system could include the following:

- Generation
- Transmission
- Information and Control Systems
- Distribution
- Substations
- Control Centers.

A list of critical physical security assets will vary with different types of ES organizations. One possible criterion for identifying critical physical assets is shown in **Attachment G.**

Critical **cyber** assets could include the following:

- SCADA (Supervisory Control and Data Acquisition) and EMS (Energy Management System)
- Plant control systems such as GDACS (Generic Data Acquisition and Control System)
- Other Interconnection systems such as Electronic Tagging, Interchange Distribution Calculator, and OASIS (Open Access Same-time Information System).

Again, a list of such assets will vary from organization to organization within the ES: a power marketing entity's list of critical cyber assets will differ from those of a high-voltage transmission entity. One possible criterion (which may not be appropriate for all ES members) is shown in **Attachment G**.

Physical Security

- Develop a critical assets list, using the queries found in **Attachment G**. Sample:

> *Public Health and Safety*
>
> Will the loss or compromise of the electrical infrastructure asset disrupt or otherwise threaten the public safety and health, and/or environment of the United States, Canada or Mexico?
>
> A few examples might include electrical infrastructure that supports:
>
> - potable water supplies,
> - sewage treatment facilities,
> - critical traffic signals,
> - critical public safety and emergency services,
> - street lights in critical areas,
> - communications facilities, and
> - severe storm tracking and warningcenters.

Cyber Security

- Develop a critical assets list, using the queries found in **Attachment G**. Sample:

> *Critical Systems*
>
> Will the loss or compromise of operational systems disrupt or otherwise threaten control of the generation, transmission, or distribution of electricity in real time.
>
> A few examples, for the case of a high-voltage transmission organization, might be the following:
>
> - SCADA/EMS Systems
> - GDACS.

Physical and Cyber Vulnerability Assessment (VA)

The selection of specific physical and cyber security VA tools and methodologies is the purview of the individual entity. The suite of tools and methodologies selected should, however, provide coverage for the entire range of **ASSURANCE, AVOIDANCE, DETECTION**, and **RECOVERY** in the model as appropriate to the needs of the organization, its customers, and the region and continent as a whole.

A strong security posture can be divided into two parts:

- Tactical security practices in place.
- Strategic security processes.

Most existing security methodologies, such as "Red Teaming"[3] deal almost exclusively with tactical issues. **When choosing a security methodology, it is extremely important to include the strategic issues.**

Tactical Issues

Sample *tactical* queries to evaluate cyber and physical vulnerabilities are listed below. See **Attachment H** for a more complete listing.

> - *Sample:* Intrusion Detection – Are intrusion detection sensors installed on all critical facilities? Are the sensors maintained and monitored? Do the sensors have a high rate of false alarms leading staff to ignore alarms? Are sensors installed in layers to raise the probability of detection?

[3] A "red team" is a team of security specialists invited in to attack physical and/or cyber systems to test security without causing damage

- *Sample:* Response – Does the enterprise have the necessary processes and protocols in place to assure as quick and effective a response by local and national law enforcement agencies and fire departments as is possible, given the distributed nature of electrical facilities? Do they run cooperative drills to familiarize law enforcement and fire departments with their facilities?

- *Sample:* Configuration Management – Does the enterprise have the tools and processes in place to assure that the configuration of computer systems is managed with security in mind? It should encompass the whole process from Development, through Testing, to Operational status. This should include documenting the need for changes (change management), design walkthroughs, code walkthroughs, controlled builds, source code management, controlled test environments, regular version releases, and a process for backing out changes if errors still creep in.

Strategic Issues

An example of a *strategic* query to evaluate cyber and physical vulnerabilities is shown below. See **Attachment H** for a more complete listing.

Sample: Management Support for Security – Does the management of the enterprise wholeheartedly support security? Do they support adequate funding for security? Do they encourage employee adherence to security policy and do they exhibit good security practices themselves?

Physical and Cyber Threat Assessment

Before an ES member can conduct a meaningful Risk Assessment, it is necessary to develop a clear, intelligence-based idea of the nature of the threats. This threat assessment is often expressed in the form of a Design Basis Threat (DBT) table (see **Attachment I** for a generic DBT for the ES). **Note:** A given threat will vary from region to region and from organization type to organization type, so this generic DBT should be tailored for each ES member.

Physical and Cyber Risk Management

Assurance includes physical and cyber risk management. Time for technological change in the information area has been dramatically dropping over the last decade: the "half life" of many products has dropped from 15 years to 5 years to 6 months, in a few cases. Many of our businesses are moving on-line in the electric industry: the move requires a whole new approach to looking at customers and managing customer relationships. Control and access to information now represents a competitive advantage, leading to a new definition of both assets and their protection requirements. As technology and business processes

change around us, so do the threats: opportunities for exploitation will continue to emerge in response to the speed at which we now live and operate.

Critical infrastructure assurance has always been recognized in industry as a risk management process. How well we manage risk—whether from market competition or from criminal or national security adversaries with malicious intent—is a function of knowledge about four elements:

- potential threats,
- vulnerabilities,
- consequences, and
- the affordability of solutions.

See **Attachment E** for more on Risk Management Approaches.

Physical and cyber security includes business procedures and controls, as well as culture, education, and policy. Many organizations have built into business management processes a periodic re-assessment of competitive threats to our business, building agility into our organization's ability to respond appropriately. The same will have to be done for physical and cyber security, particularly information security, as its importance grows in the electric industry. **Because physical and cyber security are components of electric service assurance and are tied tightly into our operational processes, no one else can do it for us.**

Problems with cyber and physical security risk management could be addressed by several means:

- The ES-ISAC could be used as a clearinghouse for information on risk management tools and processes.
- ES members could organize/acquire training in risk management.
- ES members could place security under one management chain.

Mitigation

Many people think of mitigation as the hardening of facilities (e.g., guns, gates, and guards), but mitigation is far more complex. Hardening is just one of the options available.

Physical Security

In the case of a widely distributed system (e.g., a transmission system), hardening may be prohibitively expensive and may not be very effective. Fortunately, the ES has a wide range of options available. For physical security, these options include the following:

- alternate routing of power and communications,
- strategically located spares,

- recovery procedures,
- redundancy,
- mutual assistance,
- mobile backup generation, and
- hardening.

Hardening may be called for in the case of vitally important or staffed facilities. In other cases, ES members may chose to use other options to mitigate the higher risk vulnerabilities.

Cyber Security

Mitigation for cyber systems will generally include fixing all high- and medium-risk vulnerabilities, and most low risk-vulnerabilities where those fixes are consistent with an entity's cyber security policy. The level of effort is generally low to moderate, and the cost of not getting it right far exceeds the effort involved. However, even here other options exist. These options include the following:

- redundant systems,
- automatic fail over,
- response procedures,
- response teams,
- recovery procedures,
- manual processes, and
- backup power systems.

Again, the choice of mitigation remains with the individual ES member.

SECTION II-C. DETECTION

> ➢ To protect their assets and operation, ES utilities need to carry out the following: (1) monitor cyber and physical intrusion systems; (2) monitor warnings from the NIPC, the Indications, Analysis and Warning (IAW) program, the ES-ISAC, and other sources of information; (3) conduct intelligence-gathering activities; report events via the ES-ISAC, IAW, or DOE (as appropriate), and (4) consistently follow protocols to investigate events.

Suggested Roles

Responsible Entity	Suggested Role in Detection
Utility Executives/Management	▪ Policy and Governance ▪ Leadership ▪ Commitment ▪ Resources ▪ Support
Heads of Operations	▪ Monitoring and Reporting
Heads of Physical Security	▪ Reporting of Physical Security Events ▪ Monitoring of Physical Intrusion Systems ▪ Investigation of Physical Security Events ▪ Intelligence[4] Gathering
Heads of Cyber Security	▪ Reporting of Cyber Security Events ▪ Monitoring of Cyber Intrusion Systems ▪ Investigation of Cyber Security Events ▪ Intelligence[4] Gathering

Need

Discussion

DETECTION focuses on three functions:

- organizational monitoring,
- reporting, and
- investigating.

These are carried out as responses to physical and cyber threats and to suspected or actual incidents. ES encourages individual organizations to develop and implement monitoring programs for physical and cyber security threats and incidents. These programs should also be accompanied by the development of an investigation process and the reporting of such threats and incidents to industry and/or cooperative governmental analysis and warning programs.

4 Intelligence gathering through open sources, liaison with Law Enforcement, and through interaction at public conferences and forums are a particularly useful means for a better understanding of potential adversaries, their motives, methods, and means. However, there are specific legal limitations on gathering this type of information that must be recognized and observed (e.g., limitations on information protected by privacy statutes).

Currently, real-time monitoring and reporting is needed to permit timely organizational response to threats.

Response management is a critical component of the protection program. In order to respond successfully to threats and incidents, each ES organization needs to develop, implement, and maintain a process to analyze information/reports collected from monitoring and to determine the appropriate follow-up action.

The ES-ISAC, an industry-sponsored program, was established to provide a unified means to analyze and share information. The ISAC, working with appropriate industry personnel and government agencies, will gather, analyze, appropriately sanitize, and disseminate private sector information to both industry and the NIPC. Although crucial to a successful government-industry partnership, this mechanism for sharing important information about vulnerabilities, threats, intrusions, and anomalies must not interfere with direct information exchanges between ES entities and the government.

The ES-ISAC may take as a model certain aspects of such institutions as the Centers for Disease Control and Prevention that have proved highly effective, particularly its extensive interchanges with the private and non-federal sectors. The ISAC would then possess a large degree of technical focus and expertise and non-regulatory and non-law enforcement missions. Critical to the success of the ES-ISAC will be its timeliness, accessibility, coordination, flexibility, utility, and acceptability.

The NIPC serves as the national focal point for threat assessment, warning, investigation, and response to attacks on the critical infrastructures. A significant part of its mission is to establish mechanisms to increase the sharing of vulnerability and threat information between the government and private industry.

Its first IAW initiative focuses on electric power. With the assistance of government officials and ES industry representatives, the NIPC developed general guidelines for voluntarily reporting any operational and cyber incidents adversely affecting the nation's electric power infrastructure. The initiative has two goals:

1. tactical—to warn of impending attacks or likely developments during the early stages of an attack, and
2. strategic—to warn of longer-term threats to and vulnerabilities in critical infrastructures.

The initiative seeks timely reports from industry on incidents meeting one or more of 15 predefined event criteria. ES entity personnel (physical and cyber) are responsible for incident reporting. To secure the broadest participation in the IAW program, the standard Incident Reporting Format (which features a document template) resides on and can be used to report incidents through the FBI's secure InfraGard web-server and the NERC Security Coordinator Information System. Additionally, incident reports can be sent by the

originator to the NIPC Watch & Warning Unit using the email or FAX addresses shown on the reporting form.

Some information available to the NIPC may be classified or law enforcement-sensitive and, thus, unavailable to many in the industry. A select group of NERC officials and other designated industry personnel with security clearances will be provided with the means to access and sanitize classified material. A mechanism is in place to obtain additional security clearances as required.

Training is important. NERC and the NIPC sponsored three regional workshops (one in the Western Systems Coordinating Council, one in the Electric Reliability Council of Texas, and one in the Eastern Interconnection) open to ES entities interested in participating in the information-sharing program. Each workshop provided stand-alone instruction, guidance, and materials, to enable participants to set up program operations at their facilities. Training will continue to be provided in a variety of formats to meet the industry needs.

Separately, and to sustain the indications and warning program over the longer term, NERC will consider the addition of essential elements of NIPC's IAW program to its operator training and recertification syllabus.

On July 12, 2000, the NERC Operating Committee approved the voluntary reporting through the Electric Power IAW by Control Areas, Security Coordinators, and NERC member organizations in North America.

For more detail on how the IAW initiative works, please see **Attachment J**.

Potential Solutions/Implementing Actions

- Focus on real-time monitoring of events logs or device-specific data. Cyber monitoring would include critical systems such as network management, servers, and intrusion detection/firewall systems. Physical monitoring would include surveillance systems, intrusion detection, and access control.
- **Automate Monitoring and Alerting Efforts.** The number of sources and the volume of data make this a prudent step.
- **Develop Correlation Abilities.** Be able to correlate unique events from different source logs to identify patterns that, in combination, could indicate a particularly harmful threat/incident.
- **Focus of Reporting.** Include a focus on reports from access control systems, video surveillance, voice recordings, facility inspections, reports of credible threats by employees, and external threats reported by law enforcement authorities.
- **Analyze the monitored information.**

- **Explore Participatory Reporting.** Report, as appropriate, the threat or incident to internal management, internal security organization, and external law enforcement. ES organizations may also consider participatory reporting through electric industry reliability programs (e.g., ISAC) and cooperative governmental agencies (e.g., NIPC).
- **Develop Response Team Capability.** Each ES organization should approve the formal establishment of a response team function, whether as an organizational unit or ad-hoc team. This action clearly defines the composition of the response team, its responsibilities and objectives, its internal reporting relationships, and the response process.
- **Develop Investigation Protocol.** The establishment of a well-planned formal investigation protocol will ensure that each threat and/or incident is investigated in a consistently thorough method. The investigation protocol should discuss documentation requirements, evidence collection process, evidence preservation requirements, chain of custody requirements, accepted methods of conducting personal interviews, the use of available analytical tools, and a plan for periodic tests and update of the investigation protocol.
- **Develop Reporting Requirements.** Each ES organization needs to determine under what conditions threat and/or incident information will be reported to external law enforcement agencies, the ES-ISAC, the NIPC's IAW, or some other external reporting program. The factors that will influence this decision should be documented before an investigation is recommended. Obvious factors include the seriousness of the threat/incident, likelihood of successful prosecution, an unsolvable incident, a violation of federal and/or state law/regulation, organizational policy, impact on the ES industry, impact on other critical infrastructures, and potential "costs" of the disclosure.
- **Notification and Coordination with Law Enforcement.** Each ES entity needs to develop an organizational policy (if none exists) that defines under what conditions they will notify external law enforcement and the protocols that they will use to coordinate with them. Special factors, in addition to those listed above, include internal security capability, organization structure, previous practices, and external law enforcement protocols and contacts.
- **Insider Threat.** Each ES entity needs to develop (if it has not already done so) organization policy and protocols for dealing with the insider threat (see **Section III-B**, Insider Threat).
- **Information Sharing.** The ES-ISAC has been established by NERC. Broad participation of individual ES organizations in the development and operation of the ISAC is vital for the ISAC to meet its industry objectives (see the end of **Section II-A**, ES-ISAC).

SECTION II-D. RECOVERY AND RESTORATION

- To protect their assets and operation, ES utilities need to have business recovery plans in place. They should participate in a utility mutual assistance program, and conduct periodic simulation tests. They should also have a mechanism in place to feedback Lessons Learned within their own entity and, preferably, within the whole ES.

Suggested Roles

Responsible Entity	Suggested Role in Recovery and Restoration
Utility Executives/Management	▪ Policy and Governance ▪ Leadership ▪ Commitment ▪ Resources ▪ Support
Heads of Operations	▪ Execute Business Recovery Plans ▪ Initiate Mutual Assistance ▪ Participate in Simulation Testing of Recovery and Restoration Processes ▪ Feedback Lessons Learned
Heads of Physical Security	▪ Participate in Simulation Testing of Recovery and Restoration Processes ▪ Participate in Execution of Business Recovery Plans ▪ Feedback Lessons Learned
Heads of Cyber Security	▪ Participate in Simulation Testing of Recovery and Restoration Processes ▪ Execute Cyber Business Recovery Plans ▪ Feedback Lessons Learned

Need

The ES is very good at physical recovery and restoration, because it has dealt with natural disasters year after year. Many ES members will already have some of the necessary pieces in place, such as formal and informal utility mutual assistance programs. Other parts such as simulation testing of recovery and restoration from physical attack will be only slightly different from the current simulation testing that they may do for earthquake and other natural causes. Some other parts, such as business recovery plans following a deliberate

attack, will need to be developed or may perhaps be adapted from business recovery plans developed for Y2k. As a result, for most ES members this will be a case of building on what they already have in place, rather than starting from scratch.

Formalized Utility Mutual Assistance

In addition to informal agreements among utilities, two principal utility organizations have formalized mutual assistance procedures for recovery following a major outage: the Mutual Emergency Material Support, and the Edison Electric Institute's Mutual Assistance Program.

Mutual Emergency Material Support (MEMS)

Electric utilities in the Southeastern U.S. founded the Mutual Emergency Material Support (MEMS) following the landfall of Hurricane Hugo in 1989. Intermat, Inc. operates MEMS for a voluntary group of approximately 75 electric utilities. Members of this association have agreed to aid each other during emergencies, equipment failure, or other crises that unexpectedly interrupt electrical service. This “sharing” of inventory allows member utilities to reduce inventory costs while having enhanced access to the materials they might need in the wake of disaster.

Electric utilities, electrical equipment manufacturers, and equipment vendors have created individual equipment and parts identification systems, often identifying similar or identical parts by different numbers and names and/or descriptions. Under the MEMS agreement, Intermat developed and now maintains an extensive database that cross-references the stock numbers and parts names.

In addition, the MEMS group of utilities regularly meets to exchange ideas about better business practices in the utility industry

Edison Electric Institute - Mutual Assistance Program

The Edison Electric Institute (EEI) offers another mutual assistance program. Under the EEI procedures, member organizations can request emergency assistance from other member organizations in the form of personnel or equipment to aid in restoring electric service following natural disasters, equipment malfunctions, accidents, or sabotage. The EEI has established suggested principles that have served as the basis for formation of contract standards when emergency assistance is required. While response to emergency assistance requests is voluntary, actual experience indicates that member organizations will provide such assistance when personnel and equipment are available.

The pre-established contract and operating principles developed by EEI simplify and reduce the contracting process between the Requesting and Responding utilities. The areas where EEI has established suggested principles include the following:

- guidelines on when personnel and equipment expenses commence;
- supervision and record-keeping requirements;

- definition of what personnel and equipment expenses are reimbursable and guidelines on when reimbursement payments should be expected;
- guidelines concerning liability and indemnities;
- various insurance, workers compensations, and medical expense information; and
- specifications concerning a description of what repair work is to be undertaken and what personnel, equipment, and related information are to be provided by the Requesting and Responding utilities.

Cyber Threats & Terrorism

The severity of effects from natural disasters provides a ready parallel for the severity of effects from deliberate human actions. Electric utilities must also prepare for restoration after human-caused events such as vandalism, theft of critical components, sabotage, terrorism, and cyber attacks. Vandalism and theft have been with the industry since the beginning; sabotage has been a concern primarily during wars. However, increased use of computer controls and technology have made cyber threats an increasing concern for individual electric utility, power pool, and area power coordinating council operations.

Vulnerabilities are magnified by the way the electric system is now managed:

- Computer control of power system facilities, and/or
- information posted on public telecommunications networks.

Several conditions make the threat of misuse of utility control systems by *insiders* a concern for electric utilities. This concern arises because:

- Most electric utility computer operations are accessible only to utility personnel operating within utility control centers, power plants, or substations.
- The use of open systems within organizations to facilitate information exchange exposes those systems to threats from personnel (employees, vendors, and contractors) who have internal system access rights.
- Individuals possess specific technical knowledge, including means to defeat security measures to manipulate or disrupt operations.

However, outsider threats—for instance, denial of service and Trojan Horse types of attacks—have also already adversely affected utility operations. Interference in SCADA systems could cause power outages and pose a safety hazard to utility line maintenance personnel. Denial of access to utility websites and/or the Internet potentially interrupts the sale and purchase of electricity. These threats are serious, and increasing.

Problems

Development of Business Recovery Plans

After an incident, ES utilities must restore both electrical service to customers and normal utility business activities. In the emerging competitive electricity market, a lengthy disruption of business operations can have serious impacts on an organization's ability to remain profitable and stay in business. **ES organizations must focus on both the cyber and physical aspects of business operations recovery.**

Cyber

Cyber systems are a large part of the business operations for members of the ES. Virtually all ES organizations rely on computerized systems for customer billing, for system operation, and for internal organization management functions. Where competitive market bids for power exchanges must be prepared, the reliance is even heavier and more time-critical. A plan to restore business operations following a cyber disruption incident could mean the difference between business success and failure, even in the short term. Cyber systems are becoming steadily more important in the day-to-day operation of the electrical system. Business recovery plans for the aftermath of a cyber disruption are necessary.

Currently, a significant number of ES members have "business continuity plans" developed as a part of the Y2k planning effort. Although not designed specifically to counter cyber attacks, they offer a good baseline for the business recovery planning process. Utilities with these plans in place need only review them and make any necessary modifications to cover situations involving intentional attacks. Some plans may also need to be updated to reflect any new situations. Other ES members will need to begin developing business recovery plans to keep from having to develop their procedures in the midst of a disruption incident. The models from the Y2k planning effort can be a significant resource as these plans are prepared.

The existing problems in the business recovery planning process for cyber systems can be summarized as follows:

- Few ES members have business recovery and/or business continuity plans in place that deal specifically with intentional attacks on cyber systems. Few of the plans address issues such as:
  - coordinated attacks on multiple cyber systems,
  - attacks focused on data corruption or alteration,
  - attacks designed to gain unauthorized access to business-proprietary information, and
  - attacks designed to assume malicious control and operation of the ES.
- Business recovery plans that do exist focus on natural disasters or equipment failures: one-time events with a definitive endpoint. They do not address the need

to actively contain and terminate deliberate disruptions and sustained attacks that may continue and be repeated over an extended period of time.

- Recovery plans that do exist lack sufficient elements to aid both organization officials and law enforcement personnel in the identification, apprehension, and prosecution of perpetrators. Potential conflicts between law enforcement objectives and business recovery objectives (i.e., preserving evidence to help catch the perpetrators vs. quick system recovery) need explicit attention.
- NERC provides oversight and technical advice on recovery only for the bulk power systems. There is no comparable support for distribution system recovery planning.
- Business recovery plans frequently do not include investment in redundant cyber systems and backups that could be brought into operation quickly and with a minimum of system down-time.
- ES members that do have business recovery plans often do not have a systematic process in place to keep these types of plans up-to-date.
- Few ES members have public affairs communications plans in place to manage damage control, in case cyber security is compromised.

Physical

Effects from isolated intentional attacks on physical facilities (e.g., transmission lines, substations, power plants) are only marginally different from those of natural events (e.g., tornadoes, hurricanes, earthquakes). This applies to the nature of the damage inflicted and to the ability of ES members to begin repair operations.

There are, however, significant differences between natural disasters and well-planned, coordinated, and widespread intentional attacks on physical facilities. For example, attackers could focus on multiple targets simultaneously. They could deliberately target long-lead-time equipment that could leave the system handicapped for extended periods. They could deploy chemical or biological weapons to hamper repair crews and prevent timely repairs.

Currently, natural disaster business recovery plans are seldom adequately documented or maintained up-to-date. This is true, even though, in practice, utilities have had numerous occasions to exercise such plans. Further, the plans that do exist do not address business recovery procedures in the wake of well-planned or widespread malicious attacks. They also do not provide an adequate model for business recovery plans in the event of such an attack.

The existing problems in the business recovery planning process for physical systems can be summarized as follows:

- Most ES members do not have in place business recovery plans that include procedures for dealing with widespread, well-planned attacks on physical facilities. Likewise, they do not include procedures for dealing with deliberate attempts to hamper repair and restoration activities.

- As with the cyber systems, the natural disaster business recovery plans do not adequately provide for measures to aid both organization officials and law enforcement personnel in the identification, apprehension, and prosecution of perpetrators. Potential conflicts between law enforcement objectives and business recovery objectives (i.e., preserving evidence to help catch the perpetrators vs. quick system recovery) need explicit attention.
- The business recovery plans do not include investment in redundant systems, readily available spares, or backups that are adequate to maintain electric power service in the face of deliberate and extended damage or destruction of physical assets. NERC efforts to maintain industry-wide databases on locations and characteristics of key spare equipment should be expanded.
- Most ES members do not invest in physical security of all their assets, leaving much of the facilities and equipment unguarded or with only minimal protection. Security is enhanced only for selected facilities that are deemed to be at higher risk.

Periodic and Simulation Testing

The simulation of ES disruption events and the periodic testing of recovery plans are a vital part of preparedness. These activities provide an opportunity to verify the effectiveness of recovery procedures without the stress and risk of an actual emergency. These efforts need to be carried out for attacks on both cyber and physical facilities.

Cyber

The simulation of cyber disruption events and the conduct of testing of recovery plans are an immature discipline in the ES. Until relatively recently, the ability to attack cyber systems in such a way as to create major consequences has been limited. With the growing dependence on cyber systems for ES operation and the greater exposure of these systems to disruption, the procedures for conducting simulations and periodic testing of response and recovery is evolving.

The current state of ES cyber system testing relies heavily on a "Red Team" or similar technique. In this approach, an organization-supported team attempts to break into the cyber system and to determine what damage could be inflicted. The process, while effective where it is carried out, is inefficient from the perspective of increasing the security of the entire ES since, in general, only one site benefits from the results of each test.

Most cyber security audits find some subset of the deficiencies cited in **Section II-A** (AVOIDANCE). The audits and accompanying risk assessments are carried out infrequently, varying from only once per year to only whenever major systems are installed or replaced. Further, the security auditors are often seen by organization staff as the "enemy," because some have made audit results public.

The existing problems in the simulation and periodic testing of cyber system security can be summarized as follows:

- Most ES members conduct few, if any, simulations of malicious attacks. Those that carry out such simulations address only specific threats and attack scenarios (e.g., attacks that might accompany a special event such as a political convention or a sporting event) and not the broader spectrum of threats.
- The tests that are done on cyber systems generally involve a small group within the organization. Any fixes that are required are generally carried out by the information technology team. Few members of the day-to-day operational teams are trained in using the results of the simulation and testing to detect cyber attacks and respond to them.
- The testing and simulations that are done are not carried out regularly or frequently enough.
- There is little sharing of "best practices" for cyber system security among ES members.

Physical

In contrast to the testing of cyber system security, the testing of physical system security is a mature and well-understood discipline in the ES. Current practice varies from risk assessments done once every few years to risk assessments done whenever facilities are built or undergo major revamping. Reevaluations are usually done in the wake of catastrophic events that affect physical facilities. Tabletop exercises are often used to plan for earthquakes, hurricanes, tornadoes, and other natural disasters: these techniques have proven effective in testing response and recovery procedures.

In general, disruption event simulation and testing is done for natural disasters but not for malicious attacks. (The primary exception is in preparing for special events such as the Olympics.) Further, the simulation and testing is usually carried out by utility personnel with only occasional drills with local police and fire departments.

The existing problems in the simulation and periodic testing of physical system security can be summarized as follows:

- Simulation and testing is done by ES members primarily for natural disasters or equipment failures and only rarely for malicious attacks.
- Simulation and testing is generally done for single events or special occasions. There is little, if any, testing done for repeated and continuing attacks that can extend over a long period of time.
- There is little, if any, simulation and testing of cascading failure events that can begin outside a specific organization's operational domain but eventually affect the organization's operation. Simulations are almost always confined to a single organization's system.
- There is no close involvement with national, state, and local emergency management agencies in the simulation and testing exercises.

- There is little sharing of simulation and testing "best practices" among ES members.
- Depending on the outage characteristics, there may be disagreements among local governments, institutions, industries, and utilities with respect to restoration priority and rotating blackout policy.
- Few organizations have had the misfortune of needing to recover from a systemwide outage. However, preparation for a "blackstart" is needed because of the technical complexity associated with a total system restoration.
- The ES should consider whether the industry would benefit from periodic training courses on this subject for ES members

"Lessons Learned" Reporting

It is important that the "Lessons Learned" from security testing and/or actual disruption events be disseminated among ES members. Dissemination can help increase the ability of members to plan for future events. Lessons Learned from both cyber and physical events need to be disseminated.

Cyber

Under current practice, Lessons Learned from cyber security events or tests are rarely shared in any organized manner. Weaknesses that are discovered as the result of an actual intrusion may find their way into the news media. This avenue does little to increase the knowledge base from a Lessons Learned viewpoint that is useful to ES members. Reports from internal security audits, such as a "Red Team" exercise, are for the benefit of the specific organization requesting the audit and are not shared, for good reason.

The existing problems in the Lessons Learned reporting can be summarized as follows:

- No mechanism exists for gathering information on cyber security audits and sharing this in the form of sectorwide general statistics.
- There is a reluctance for ES members to report actual cyber intrusions and Lessons Learned.

With the restructuring of the electric industry, there is even less incentive for organizations to share cyber intrusion data than with the previous industry structure. A mechanism is needed to create an incentive for organizations to participate in secure information sharing among themselves.

Physical

The Lessons Learned from physical security incidents are shared among ES members to a greater extent than those from cyber security incidents, although the information is still limited. As an example, in the Western Systems Coordinating Council (WSCC) region of NERC, reports of malicious events are distributed throughout the region as a warning of potential attacks.

The existing problems in the Lessons Learned reporting can be summarized as follows:

- No mechanism exists for gathering information on physical security risk assessments and sharing this in the form of sectorwide general statistics.
- No mechanism exists for ES members to share actual physical security incidents and Lessons Learned in an anonymous context.
- With the restructuring of the electric industry, there is even less incentive for organizations to share physical intrusion data than with the previous industry structure. A mechanism is needed to create an incentive for organizations to participate in secure information-sharing among themselves.

Potential Solutions/ Implementing Actions

Approaches to addressing solutions and to providing quick and effective recovery and restoration after physical or cyber actions fall into three categories: development of Business Recovery Plans, periodic and simulations testing, and Lessons Learned reporting.

Development of Business Recovery Plans

Cyber

Some solutions to the problems defined above are as follows:

- Guidelines should be developed that outline business recovery planning procedures for cyber systems, that describe minimal and best practices, and that document experiences in the implementation of these plans. These guidelines should be in a form suitable for distribution to all ES members.
- In those rare cases where they have not already done so, ES members should be encouraged to develop business recovery plans for time-critical functions that could be seriously disrupted by an intentional attack on cyber systems (e.g., scheduling, supervisory control). These recovery plans should address the issues that differentiate an intentional disruption from those caused by natural or accidental events.
- The ES might want to consider identifying alternative mechanisms to provide oversight and support for recovery planning for distribution systems as well as for bulk power systems. The involvement of local public utility commissions in this activity should be investigated.
- Once business recovery plans are developed, all ES members that do not already do so should be encouraged to implement a regular, systematic review and updating of those plans.
- All ES members are encouraged to have communications plans in place for use if and when their cyber security is compromised.

- The ES might want to consider whether the industry could benefit from periodic training courses on this subject (education, training, and awareness) for ES members.

- Action can also be considered on the measures that state and local government organizations can use to protect against serious impacts on local residents and businesses from infrastructure disruptions.

Physical

Some solutions to the problems noted above are as follows:

- Guidelines should be developed that outline business recovery planning procedures for physical assets, that describe minimal and best practices, and that document experiences in the implementation of these plans. These guidelines should be in a form suitable for distribution to all ES members (e.g., coordinated with IEEE).
- Where they have not already done so, all ES members should be encouraged to develop, and keep current, business recovery plans that include consideration of intentional attacks on physical facilities, including attacks on multiple pieces of equipment. Once business recovery plans are developed, all ES members should be encouraged to implement a regular, systematic review and updating of those plans.
- The ES might want to consider whether the industry could benefit from periodic training courses on this subject for ES members.
- Any ES members who have not already done so should consider participation in a formal utility mutual assistance program.
- The existing NERC national inventory of spares should be updated and moved to the ISAC (see **Section III-C**, Electricity Sector Coordination).

Periodic and Simulation Testing

Cyber

Some solutions to the cyber problems noted above are as follows:

- Guidelines should be prepared on cyber security test and simulation procedures including the following:
  - development of threat scenarios to be used in testing,
  - techniques for conducting tests,
  - evaluation of test results, and
  - dissemination of Lessons Learned from the test to appropriate organization personnel.
- The ES should consider assembling and disseminating information on best practices for cyber simulation and testing from ES members. These could be made available on the ES ISAC.

- ES members should be encouraged to conduct regular cyber attack simulations and tests.
- The ES might want to consider whether the industry could benefit from periodic training courses on this subject for ES members.

Physical

Some solutions to the physical problems noted above are as follows:

- Guidelines should be prepared on physical security test and simulation procedures that focus on deliberate and malicious events including the following:
  - development of threat scenarios to be used in testing,
  - techniques for conducting tests,
  - evaluation of test results, and
  - dissemination of Lessons Learned from the test to appropriate organization personnel.
- The ES should consider assembling and disseminating information on best practices for physical attack simulation and testing from ES members. These could be made available on the ES ISAC.
- ES members should be encouraged to conduct regular physical attack simulations.
- All ES members are encouraged to include Federal Emergency Management Administration (FEMA), state, and local emergency management agencies in all appropriate security exercises.
- All ES members are encouraged to conduct frequent drills with local police and fire departments at critical facilities.
- ES members should be encouraged to establish restoration priority and rotating blackout policies in cooperation with local governments to cover different outage situations.
- ES members should be encouraged to prepare and/or update "blackstart" procedures and to conduct appropriate drills and simulations.
- The ES might want to consider whether the industry could benefit from periodic training courses on this subject for ES members.

"Lessons Learned" Reporting

It is important that the Lessons Learned from security testing and/or actual disruption events be disseminated in a timely manner among ES members. Dissemination can help increase the ability of members to plan for future events. Lessons Learned from both cyber and physical events need to be disseminated.

Cyber

Some solutions to the cyber problems noted above are as follows:

- The ES may consider developing a mechanism to compile statistical data from ES member cyber security audits. These could be posted in a secure manner on the ES-ISAC for the education of ES members.
- The ES may consider developing a Lessons Learned report following an actual cyber intrusion. This could be prepared under anonymous conditions, and a limited summary of it could be posted in a secure manner on the ES-ISAC for the education of ES members. The existing NERC cyber intrusion database could be modified to meet these conditions.

Physical

Some solutions to the physical problems noted above are as follows:

- The ES may consider developing a mechanism to compile statistical data from ES member physical security audits. These could be posted in a secure manner on the ES ISAC for the education of ES members.
- The ES may consider developing a Lessons Learned report following an actual physical security incident. This could be prepared under anonymous conditions and a limited summary of it could be posted in a secure manner on the ES ISAC for the education of ES members.

PART III: RELATED ISSUES

➲ *Part III addresses associated issues crucial to the smooth working of the plan: research and development, legal and regulatory issues, and electric power sector coordination.*

SECTION III-A. SUPPORT AND PROMOTION OF RESEARCH AND DEVELOPMENT

Current ES research and development (R&D) efforts are not currently adequate to address the new CIP challenges documented in Parts I and II. Meeting these challenges will require

- new resources,
- a new examination of R&D requirements and gaps in the context of the ES security model (AVOIDANCE, ASSURANCE, DETECTION, and RECOVERY), and
- partnership among government, industry, and academia.

Existing R&D Problems

By comparing ES vulnerabilities with ongoing R&D, a number of problems and shortfalls have been identified, as follows:

- **Inadequate Information to Determine Susceptibility to Disruption of the Energy Infrastructure**

  The following are areas that warrant further discussion and analysis:

  – Action aimed at developing a credible, comprehensive, and tested set of methodologies, databases, and tools available for use by the ES to systematically identify critical assets; conduct vulnerability assessments; carry out critical consequence analyses; and evaluate the public health and safety, economic, and social impacts of infrastructure disruptions. Some tools have been and are being developed, and some are being applied, but these are not widely accepted or used by the private sector.

  – Action oriented toward testing the applicability and reliability of vulnerability assessment tools in private sector use.

  – Action designed to systematically evaluate the energy infrastructure susceptibility on regional or national scales that transcend the boundaries of a single energy entity.

- **Lack of a Coordinated Process to Collect and Distribute Threat Information**

  There is insufficient research:

  - into the institutional and legal barriers that inhibit exchange of threat information among private sector energy entities, and between private entities and Federal, state, and local government organizations.
  - into developing secure communication mechanisms that industry and government can use to rapidly communicate threat information between private sector energy entities and federal agencies.

- **Inadequate Response and Recovery Procedures and Technology**

  There is only limited research:

  - on energy sector specific sensors and detectors suitable for detecting and mitigating physical and cyber disruptions.
  - aimed at integrating and analyzing data and information from different sensors, detectors, and other sources to make rapid determinations of the magnitude of an emergency, either physical or cyber.
  - on mitigation technology that is specific to the energy sector and that can reduce the impacts of disruptions on the energy infrastructure.

- **Interdependence of Electric Power Infrastructure and Other Infrastructures**
  - Insufficient research is being performed to develop tools that can be used on organization-wide, regional, and national scales to adequately study the interdependence of different infrastructures.

- **Gaps in Physical Protection for Energy Infrastructure Facilities**
  - There is insufficient research aimed at applying enhanced physical security technology for critical components of the energy infrastructure.
- **Limited Cyber Security for Real-Time and Energy Management Systems (EMS)**

  There is insufficient research:

  - designed to identify the particular vulnerabilities of Real-Time and EMS systems and to develop hardware and software to reduce or eliminate those vulnerabilities. Some research is being carried out by the private sector, but the results are not generally available to all Real-Time and EMS system operators.
  - into mitigation technologies that can reduce the impact of a disruption of Real-Time and EMS systems.
- **Inadequate Protection of Energy-related Information**

  There is insufficient research:

  - designed to identify the means to secure the increased information that will be required to operate the energy infrastructure, particularly the electric power system, in a deregulated environment.

  - into evaluating the energy infrastructure information that is publicly available (e.g., on the Internet) and determining its potential impact on system security.

- **Reliance on Unique, Hard-to-Procure Equipment and Materials**
  - There is insufficient effort to systematically identify critical energy infrastructure equipment and materials that are unique and hard to procure, to identify available suppliers, and to map out alternative strategies to deal with a potential loss of this equipment and/or material.
- **Susceptibility to Cascading Failures Due to Interdependencies**
  - There is insufficient research underway designed to assess the possibility and magnitude of cascading failures in the energy infrastructure due to interdependencies with other infrastructures.
- **Reliance on Rapid Access to Accurate Information**
  - There is insufficient research underway to assess the vulnerabilities of the energy infrastructure to disruptions in information flow. Such disruptions can create serious economic impacts by simply slowing down the flow of necessary data and communication.

Potential Solutions

Some solutions to these CIP-related R&D problems are as follows:

- The ES should work with government and other industry organizations to:
  - Develop a coordinated and cohesive CIP R&D program that meets the needs of the ES.
  - Develop CIP R&D priorities.
  - Define CIP R&D resource requirements.
  - Define appropriate public and private-sector CIP R&D responsibilities and technology transfer mechanisms.
  - Coordinate, as appropriate, with other sector industries.
- Develop a mechanism to collect newly identified R&D needs and bring them forward to other appropriate entities for action. NERC, as the designated Sector Coordinator, should serve the role of this central collection mechanism.
- Conduct research and develop technologies and methodologies (e.g., databases, analytical tools, software, hardware) that increase the understanding of the threats to energy infrastructure reliability, including natural, accidental, and deliberate threats.
- Conduct research and develop technologies and methodologies that can be used to conduct vulnerability and risk assessments of the energy infrastructure and to

promote the widespread application of those technologies and methodologies by the private sector and by state and local government organizations.

- Conduct research and develop technologies and methodologies that can reduce and/or eliminate vulnerabilities in the energy infrastructure.
- Conduct research and develop technologies and methodologies that can be used in the energy infrastructure to detect the onset of, reduce the impacts of, and improve the ability to recover from a disruption incident.
- Identify steps that can be taken to enhance the adoption by the private sector and by state and local government organizations of best management practices that utilize infrastructure protection technologies and methodologies.

SECTION III-B. LEGAL AND REGULATORY ISSUES

Legislative and Regulatory Goals

Potential Solutions/Implementing Actions

The following legislative goals are proposed.

- Statutory protections from public disclosure of sensitive or critical information:
  - for threat-sensitive information that is voluntarily disclosed to the federal government;
  - for economically or competitively sensitive information that is voluntarily disclosed to the federal government; and
  - for threat-sensitive (or economically/competitively sensitive) information that is disclosed pursuant to state and/or federal regulatory or statutory requirement (*example*: system maps or other indicia of the location of sensitive/critical facilities, or requiring financial disclosures to include specific or detailed data about threat risks).
- Protection from those over-intrusive government interferences in private affairs styled as infrastructure-protection law-enforcement efforts (*example*: administrative subpoena powers).
- Legislative recognition of the validity of, and protection against government intrusion into, private/voluntary efforts to increase security by means of Public Key Infrastructure (PKI) technology.
- Increased government internal coordination and external cooperation, to promote efficiency in (and reduce costs of) all aspects of both physical and cyber security efforts: prevention, detection, and remediation.

- Legislative recognition of the validity of requiring or including contractual clauses related to infrastructure protection needs.
- Federal program to assist in the private creation of strong standards for software solutions to security needs.
- Regulatory recognition to the cost of implementing a CIP program.
- Provide legal protection for the sharing of CIP information similar to the 1998 Y2k Information and Readiness Disclosure Act.

See **Attachment K.**

Legal Issues and Challenges

Problem

Legal issues and challenges are associated with cyber security risk management activities. Some of these impede industry and cross-sector cooperation; other involve legal risks that may undermine common-sense strategies. Large overarching issues include clarifying government/industry relationships with respect to critical infrastructure protection, resolving potential conflicts between federal and state regulatory policy, tax issues and incentives, etc.

As a starting point, there are four primary areas of concern:

- **Information-sharing between the Critical Infrastructure entities and the Federal government**. This information exchange raises challenges with respect to government obligations under the Freedom of Information Act ("FOIA"). FOIA creates a general presumption that information in the possession of the Federal government should be available to the public, with limited exemptions allowing for certain information to remain confidential. Although there are over 80 FOIA exemptions throughout the body of U.S. law, it is presently unclear that any of the existing FOIA exemptions would provide the certainty of protection that private industry requires for voluntary exchange of threat and vulnerability information. Some protection for critical infrastructure entities could be provided by that amended FOIA; however, it is unlikely that any such legislation would protect all information provided. (This was the intent of the 1998 Y2k Information and Readiness Disclosure Act, which supported the voluntary exchange of information.)

  The business community must be able to articulate (1) what barriers exist to effective management of cyber security, (2) how these barriers affect the private sector's ability to work with the government, and (3) what protections and incentives must be available to business to support and encourage cooperation and workable practices for voluntary disclosure of threat and vulnerability information between industry and the government.

Conversely, when the Federal government exchanges information with private industry with respect to threats and vulnerability, there may be constraints on sharing this information outside the U.S. This presents obvious issues for U.S. multinational organizations with operations outside the U.S. and for information exchange programs that are open to both domestic and foreign participants. This issue is particularly relevant and critical to North America's electric industry, as electric system reliability depends upon the security and reliability of the integrated power systems in both the U.S. and Canada.

- **Federal and state antitrust laws and practices.** Antitrust laws and regulatory practices may challenge the sharing of certain types of information between competitors or potential competitors. Antitrust laws potentially affect a wide range of cyber security management activities. Certain types of agreements, cooperative arrangements, and information-sharing among industry participants may have anti-competitive effects in areas such as pricing or output. Because the electric power sector is high-profile and often politically charged, mere cooperation among industry organizations may raise questions with a variety of regulators, consumer organizations, politicians and others—significantly increasing the risks of participation.

  Both the Federal Trade Commission and the Department of Justice understand that cooperation may actually further competition and make good business sense. Both agencies have carefully developed and issued several Joint Statements of Antitrust Enforcement Policy clarifying issues of cooperation among competitors in several areas (licensing of intellectual property, health care joint ventures, collaboration and joint ventures among competitors). These Statements explicitly spell out what types of activities fall within a "safe harbor" of acceptable activities as well as those activities that are violations of the antitrust laws from the regulator's perspective. Another possible legislative approach currently exists in the form of statutes: it addresses cooperative research and development in the energy and other sectors such as the National Cooperative Research Act.

  In 2000, after reviewing the business practices described by EPRI for its Enterprise Infrastructure Security program (a collaborative information-sharing program), the Department of Justice (DoJ) issued a favorable Business Review response that provides some limited guidance in the area of intra-sector information exchange. However, regulators have issued no safe harbors or voluntary guidelines that could serve as additional guidance for critical infrastructure organizations that want to use other means to share information with respect to cyber security risks. (For example, the DOJ issued Antitrust Guidelines for the Licensing of Intellectual Property.)

- **Emerging civil liability**. What is an organization's liability for mistakes in cyber security? What should be recognized as appropriate due diligence standards for assessing corporate and management responsibility for the protection of

information assets when damage or losses are incurred as the result of a breach of cyber security? Court opinions, tort law, and legislation currently provide no definitive legal guidance in this area. This liability presents complex issues ranging from the impact of the privacy provisions of the Gramm/Leach/Bliley cyber security regulations beyond the financial services sector to potential limitations on liability for downstream harm from cascading impact in critical infrastructure industries.

Most legal practitioners that have looked at the issue agree that there are significant gaps in the law with regard to liability. Industry, the courts, and the legislature all have a role in developing appropriate public policy, guidance, and solutions for encouraging organizations that provide critical services to improve the robustness and security of the infrastructure.

- **Legal challenges with respect to international law and activities of multinational organizations.** Cyber-security needs to be addressed from a global perspective. However, to date no international legal consensus has been achieved.

Potential Solutions/Implementing Actions

Addressing these concerns includes developing generally accepted security principles for the electric power and other sectors that can serve as legal standards of behavior for tort liability, the possibility of limited liability under certain circumstances, etc. In the area of cyber security, protection from liability would enhance the ability to perform effective risk assessments, test infrastructure security and share certain threat and vulnerability information. There are also corporate liability issues related to more traditional issues such as privacy.

Insider Threat

Problem

Cyber

Potential insider threats that the ES faces are as follows:

- Foreign nationals employed as programmers doing work for U.S. organizations.
- Vendors with access to control systems for transmission and plant operation systems.
- Employees engaged in labor disputes.
- Employees seeking financial gain.
- Employees bent on causing harm or demonstrating their ability to overcome the system.
- Employees engaged in espionage.
- Employees subject to workforce reductions.
- Former employees.

- Disgruntled employees.

See **Attachment L** for examples of recent cyber incidents.

Workplace Liability and Employee Safety

At least four organizations have been successfully sued or are being sued for failing to properly screen applicants who turned violent on the job. See **Attachment L** for these examples.

Litigation and the rising cost of for such suits, however, is only part of the picture. In fact, employee safety—not cost—may be the major issue. Public safety and, by extension, employee safety, is also one of the major focuses of PDD-63. The American public wants to feel safe in the workplace. These lawsuits may be characterized as a way to punish those employers who have placed them and their loved ones at risk.

Potential Solutions/Implementing Actions

Some possible solutions are to follow industry best practices such as the following:

- Organizations should consider verifying past employment history.
- Organizations should consider carrying out criminal background checks on all potential new hires for sensitive positions.
- Organizations should consider carrying out periodic (preferably annual) criminal background checks on existing employees in sensitive positions.
- Organizations must develop a zero tolerance policy against violence in the workplace.
- Line managers should be alert to changes in employee behavior that could be warning signs of potential problems.
- A well-designed intervention program can be effective in reducing or eliminating problems in their early stages.

SECTION III-C. ELECTRICITY SECTOR COORDINATION

> "Surprise, when it happens to a government, is likely to be a complicated, diffuse, bureaucratic thing. It includes neglect of responsibility but also responsibility so poorly defined or so ambiguously delegated that action gets lost. It includes gaps in intelligence, but also intelligence that, like a string of pearls too precious to wear, is too sensitive to give to those who need it. It includes the alarm that fails to work, but also the alarm that has gone off so often that it has been disconnected. It includes the unalert watchman, but also the one who knows he'll be chewed out by his superior if he gets higher authority out of bed. It includes the contingencies that occur to no one, but also those that everyone assumes somebody else is taking care of. It includes straightforward procrastination, but also decisions protracted by internal disagreement. It includes, in addition, the inability of individual human beings to rise to the occasion until they are sure it is the occasion—which is usually too late. (Unlike movies, real life provides no musical background to tip us off to the climax.) Finally, as at Pearl Harbor, surprise may include some measure of genuine novelty introduced by the enemy, and possibly some sheer bad luck.
>
> The results, at Pearl Harbor, were sudden, concentrated, and dramatic. The failure, however, was cumulative, widespread, and rather drearily familiar. This is why surprise, when it happens to a government, cannot be described just in terms of startled people. **Whether at Pearl Harbor or at the Berlin Wall, surprise is everything involved in a government's (or in an alliance's) failure to anticipate effectively.**"
>
> *Thomas C. Schelling,*
> *Forward to Pearl Harbor; Warning and Decision,*
> *by Roberta Wohlstetter [emphasis added]*

Problem

Interconnectedness among ES organizations is an increasing given. However, ES interconnectedness extends beyond, to many other parts of the society and economy, both public and private. Failure to include these links in the four-tiered approach to securing the CIP will result in a plan riddled with gaps.

Potential Solutions/Implementing Actions

To be effective and to survive over the longer term, CIP initiatives must reach out and involve **all entities with a stake in the outcome:** not only the organizations themselves (including their customers and shareholders), but also state/local/federal regulators and

emergency planners. These latter entities are important because potential risks and cost consequences to the organization alone do not reflect the entire cost to the region in which that organization operates. Viewed as a commodity, energy is only one input of many needed by other industries to manufacture products or provide services for their customers. Thus, in a business sense, there is a multiplier effect between the risks and cost consequences that accrue to the affected energy organization and to those for the entire region served by that organization.

Such multiplier effects from a given service disruption may be very different between regions.

- *Example:* A region that is predominantly agricultural may have a noticeable energy multiplier effect only during certain seasons of the year (e.g., planting, harvesting).
- *Example:* Another region comprised largely of manufacturing and heavily energy-intensive industries may have an extremely large energy multiplier effect regardless of the season.

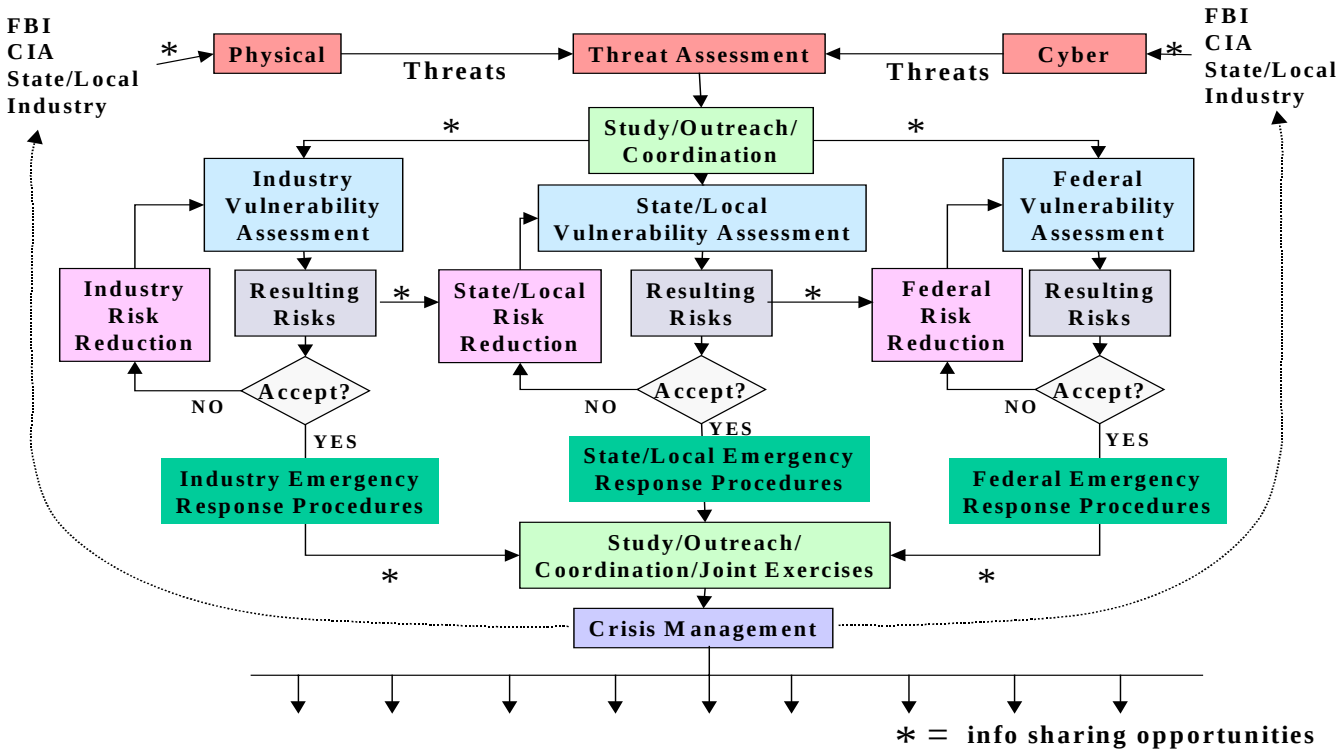
The point (the potential problem) is that the energy entity neither sees nor has incentives to insure against these additional cost consequences.

Figure 2 (Overall Concept of Operations) presents one concept for a meaningful involvement of all stakeholders. It depicts **a conscious effort** on the part of all agents (i.e., sector entities, state/local/Federal planners) to **identify** potential threats and incidents, both physical and cyber, and then to **coordinate** risk reduction and consequence management preparations accordingly. Using an information- and risk-sharing approach, each agent would pursue risk reduction objectives and integrate them with the emergency plans and risk reduction initiatives of each of the others. Such coordinated planning would assure that all pertinent emergency events are considered, practical solutions are developed, regulatory matters are addressed, and a workable crisis management plan exists to deal with residual risk consequences.

An additional advantage of this approach is that each agent will better understand the level of preparedness built into critical infrastructure systems and, therefore, the type and extent of additional emergency measures that may be prudent. It is possible, after all, to exacerbate the consequences of an emergency by responding improperly—in spite of preparedness and risk reduction initiatives that may already be in place.

ES members should begin immediately to set up a national inventory of long lead-time electrical system spares, kept secure by NERC, as part of the ISAC. The ES members should negotiate the necessary protocols in advance, so that those spares could be accessed quickly in an emergency. This will require that NERC host a secure, up-to-date directory of key ES contacts for this and any other coordination needs that will develop as CIP is better defined.

Figure 2. Overall Concept of Operations



SECTION III-D. CONCLUSION

This paper identifies a number of physical and cyber security challenges and potential actions that an ES member organization may want to consider. Because each organization has different organizational needs and concerns, not all of the potential actions/solutions outlined may address its particular situation. Each organization may already have some of these elements in place. However, four areas stand out as being most in need of additional investigation or special care:

- **Interdependencies** – The interdependencies between the ES and other industries, such as telecommunications, and other energy industries such as natural gas, are not well understood. The ES, oil, natural gas, and coal industries, as well as the other sectors, should participate in regional interdependency simulation exercises to gain a better understanding of how the industries interact. The value of such tabletop exercises was recognized in the late 1980s by the National Electric Security Committee formed by NERC at the behest of the United States government's National Security Council, as it addressed an increase in state-sponsored global terrorism. It was recognized again in 2000 with the Black Ice interdependency exercise for the Salt Lake City Winter Olympics. The ES may find it necessary to take the lead in assuring that such exercises are conducted.

- **Insider Threat** – Many ES members already have processes in place, but the insider threat is significant and difficult to address, and will require increasing attention.

- **ES ISAC –** To facilitate information sharing of physical and cyber threats within the industry and among other critical infrastructures, NERC has developed an Electricity Sector Information Sharing and Analysis Center, is partnering with the National Infrastructure Protection Center, and is participating in outreach activities. All industry organizations are encouraged to participate in this information-sharing program.

- **Cyber Security** – Cyber security is fast becoming a bigger issue for ES members, as a consequence of the rapidly evolving cyber threat, coupled with the widespread use of Internet based applications. Even ES members who have outstanding cyber security programs should not be complacent, but should regularly re-examine and improve those programs in the face of the rapid pace of change.

GLOSSARY

Access	Opportunity to make use of an asset.
Access control	Systems and processes that limit access to assets and resources to authorized individuals and processes only.
Accountability	The principle that responsibility for ownership and/or oversight of an asset or resource is explicitly assigned and that assignees are answerable to proper authorities for stewardship of assets and resources under their control.
Application	A software package designed to perform a specific set of functions. See also **Program**.
Asset	Any information, facilities, objects, people, processes, systems, capabilities, etc., that have value to the organization or that can damage the organization's capability to meet its goals or accomplish its mission.
Attack	An intentional attempt to bypass the physical or cyber security measures and controls protecting an asset.
Audit	An independent review and examination of security systems and processes, records, and activities to assess the adequacy of system controls, to assure compliance with established security policies and procedures, and/or to recommend necessary changes in system controls, policies, or procedures to meet security objectives.
Availability	Timely, reliable access to electrical service or information for authorized individuals or processes.
Blackstart	The process of restoring electrical service to a control area or region after it has experienced a total loss of electrical power.
Business recovery plans	Documented procedures for continuing to conduct business during an event(s) that disrupts normal business processes.
Capability	The tools, techniques, tactics, forces, etc. by which a cause produces an event.
Cause	The initiating person, action, or thing that facilitates the occurrence of an event.

Change control	See **Configuration management.**
Client-server architecture	An architecture consisting of server programs that await and fulfill requests from client programs on the same or another computer.
Code	In computer programming, a set of symbols used to represent characters, format commands, and instructions in a program. **Source Code** refers to the set of commands and instructions making up a program.
Computer	A machine that can be programmed in code to execute a set of instructions (program).
Computer network	A set of computers that are connected and able to exchange data.
Confidentiality	Assurance that information is not disclosed to unauthorized persons, processes, or devices.
Configuration control	The process of controlling modifications to hardware, software, firmware, and documentation to ensure that a system is protected against improper modification before, during, and after system implementation.
Configuration management	Management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the life cycle of a system.
Consequence	The cost of an event occurring. Optimally expressed in terms of dollars, but may be a function of time (replacement, repair, lost market advantage, etc.), availability, personnel, etc.
Cracker	A person who uses a Password Cracker to gain unauthorized access to a system.
Critical Infrastructure	Physical or cyber-based system essential to the minimum operations of the economy and government.
Cyber	All of the electronic and human components involved in the collection, processing, storage, transmission, display, dissemination, and disposition of information.
Denial of Service (DoS)	Result of any action or series of actions that prevent any part of a system from providing data or other services to authorized users.

Design Basis Threat (DBT)	The temporally and spatially bounded definition of the range of possible threats against an asset or group of assets derived from a range sources, including military and law enforcement intelligence services.
Disaster recovery	The process of restoring a system or other asset to full operation after a major interruption in service.
Distributed Denial of Service (DDoS)	A denial of service attack launched from multiple sources at the same time.
Emergency response plans	Documented procedures for restoration of electrical or cyber service to customers and users following an event(s).
Event	An occurrence, not yet assessed, that may affect the performance of an asset. See **Incident.**
Firewall	An access control mechanism that acts as a barrier between two or more segments of a computer network, or overall client-server architecture, used to protect internal networks or network segments from unauthorized users or processes.
Firmware	Application recorded in permanent or semi-permanent computer memory.
Hacker	Any unauthorized user who gains, or attempts to gain, access to a system, or who denies access, or attempts to deny access to authorized users to a system, regardless of motivation.
Hardware	The physical components of a computer system.
Incident	An occurrence that has been assessed as having an adverse effect on the security or performance of an asset.
Information warfare	Actions taken to affect an adversary's information and information systems while defending one's own information and information systems during times of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.
Integrity	Condition existing when a system operates without unauthorized access, modification, alteration, impairment, or destruction of any of its components.

Intent	Relates a cause to assets by identifying what types of assets are susceptible to this cause.
Internet	A decentralized, global network of computers (Internet hosts), linked by the use of common communications protocols. The Internet allows users worldwide to exchange messages, data, and images.
Intranet	A private network for communications and sharing of information that, like the Internet, is based on TCP/IP but is accessible only to authorized users within an organization. An organization's intranet is usually protected from external access by a firewall.
Intrusion	Attacks or attempted attacks from outside the security perimeter of an asset.
Mitigation	Proactive measures implemented to mitigate the consequence of a risk.
Password	A string of characters, ideally containing letters, numbers, and other keyboard symbols that is used to authenticate a user's identity or authorize access to data. A password is generally known only to the authorized user who originated it.
Password cracker	An application that tests for passwords that can be easily guessed such as words in the dictionary or simple strings of characters, or an application that tries by brute force to cycle through all possible combinations of characters to find a password.
Probability of occurrence	The likelihood of a particular cause initiating a specific event, given a particular cause.
Program	A set of instructions in code that, when executed, causes a computer to perform a task.
Protocol	A set of rules and formats, semantic and syntactic, that allow one system to exchange information with another.
Red team	A team of cyber security specialists invited in to attack cyber systems to test cyber security without causing damage.
Redundancy	Duplication of electrical or electronic system components, information, spare parts, or personnel intended to increase the reliability of service.

Risk	The characterization of assets, and events that can affect the assets, the consequences of the events occurring, and the probability of the events occurring.
Risk assessment	An examination of the relative probability, to a physical or cyber system, of a security, safety, environmental, operational, financial, or other event. For PDD-63 purposes, we will consider only security events, although, in general, risk assessments are a much larger subject.
Risk management	The identification, assessment, and mitigation of probabilistic security events (risks) in physical and cyber systems to a level commensurate with the value of the assets protected.
Router	A device that connects two networks or network segments and may use IP to route messages.
Reliability	Providing consistent and dependable electrical service or information.
Security scanner	An application that scans passwords, patch levels, etc. to check a cyber network and systems for vulnerabilities.
Simulation testing	An exercise (typically tabletop) during which a knowledgeable interdisciplinary group works through an event or group of events.
Social engineering	The process by which unauthorized individuals manipulate unwary users or system administrators to gain access.
Software	The electronically stored commands and instructions that make an automated system functional, including the operating system, applications, and communications protocol.
Source code	See **code**.
System administrator	Person responsible for the effective operation and maintenance of a system, including implementation of standard procedures and controls to enforce an organization's security policy.
Targeting	The immediacy of a cause relative to an event and an asset.
Telecommunications	Preparation, transmission, communication, or related processing of information (text, images, sounds, or other data) by electrical, electromagnetic, light, or similar means.

Threat	Any circumstance or event that could harm an asset through unauthorized access, compromise of data integrity, denial or disruption of service, or physical destruction or impairment.
User	A person or process authorized to access a system.
Virus	A small, self-replicating, malicious program that attaches itself to an executable file or vulnerable application and delivers a payload that ranges from annoying to extremely destructive.
Vulnerability	A flaw in facilities, security procedures, software, internal system controls, or implementation of a system that may affect the safety, operation, integrity, confidentiality, accountability, and/or availability of an asset. For PDD-63 purposes we will only consider flaws that may be deliberately exploited, although in general, vulnerabilities include flaws that may cause failure due to inadvertent human actions, natural disasters or other causes as well.
Vulnerability assessment	An examination of the ability of a physical or cyber system, including current security procedures and controls, to withstand assault. A vulnerability assessment may be used to: (1) identify weaknesses that could be exploited; and (2) predict the effectiveness of additional security measures in protecting physical and cyber assets from attack.
Vulnerability audit	The process of identifying and documenting specific vulnerabilities in physical or cyber systems.
War dialer	An application that brute force cycles through a range of phone numbers looking for a modem tone.
Web site	A location on the World Wide Web, accessed by typing in its address (URL) into a Web browser. A Web site always includes a home page and may contain additional documents or pages. See **World Wide Web**.
World Wide Web (WWW)	A system of Internet hosts that support the exchange of messages, textual documents, and audio, video, and graphics images. See **Internet**.

ACRONYMS

ADA	Americans with Disabilities Act
AGC	Automatic Generation Control
CALEA	Communications Assistance for Law Enforcement Act
CEO	Chief Executive Officer
CERT	Cyber Emergency Response Team
CFO	Chief Financial Officer
CIAO	Critical Infrastructure Assurance Office
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIPWG	Critical Infrastructure Protection Working Group
COO	Chief Operating Officer
DARPA	Defense Advanced Research Projects Agency
DBT	Design Basis Threat
DDoS	Distributed Denial of Service
DoD	Department of Defense
DOE	U.S. Department of Energy
DoJ	Department of Justice
DoS	Denial of Service
DTF	Dispatcher Training Facility
EEI	Edison Electric Institute
EMS	Energy Management System
EPRI	Electric Power Research Institute
ES	Electricity Sector
ES-ISAC	Electricity Sector Information Sharing and Analysis Center
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Administration
FERC	Federal Energy Regulatory Commission
FOIA	Freedom of Information Act
FRP	Federal Response Plan
GDACS	Generic Data Acquisition and Control System
IAW	Indications, Analysis and Warning
IEEE	Institute of Electrical and Electronic Engineers
ISAC	Information Sharing and Analysis Center
IT	Information Technology
kWh	kilowatthour

MEMS	Mutual Emergency Material Support
MW	megawatt
NERC	North American Electric Reliability Council
NIPC	National Infrastructure Protection Center
NIST	National Institute of Science and Technology
OASIS	Open Access Same Time Information System
PC	Personal Computer
PCCIP	President's Commission on Critical Infrastructure Protection
PDD	Presidential Decision Directive
PKI	Public Key Infrastructure
PMA	Power Marketing Administration
R&D	Research and Development
RA	Risk Assessment
SCADA	Supervisory Control And Data Acquisition
SCIS	Security Coordinator Information System
SDWT	Self Directing Work Team
SO	Standing Order
SOP	Standard Operating Procedure
TCP/IP	Transmission Control Protocol/Internet Protocol
VA	Vulnerability Assessment
VERT	Virus Emergency Response Team
WSCC	Western Systems Coordinating Council
WWW	World Wide Web

MEMBERSHIP

Stuart Brindley
Acting Director, Information Technology and Infrastructure
Independent Electricity Market Operator
Station A Box 4474
Toronto ON M5W 4E5
Phone: (905)-855-6108
Cel: (416)-606-1250
Fax: (905)-855-6471
E-mail: stuart.brindley@theIMO.com

Ed Chittester
Electrical Engineer
Bonneville Power Administration
Post Office Box 491 M/S TOS
Vancouver, Washington 98666-0491
Phone: (360)-418-2320
Cel: (360)-241-0128
Fax: (360)-418-8186
E-mail: eschittester@bpa.gov

Glen Coplon
Lead Staff
The MITRE Corporation
1820 Dolley Madison Blvd. M/S W422
McLean, Virginia 22102-3481
Phone: (703)-883-6561
Fax: (703)-883-1397
E-mail: ghcoplon@mitre.org

Jim Fortune
Manager, Strategic Assessment
Electric Power Research Institute
Post Office Box 10412
Palo Alto, California 94303-0813
Phone: (650)-855-2500
Fax: (650)-855-2065
E-mail: hfortune@epri.com

Gene Gorzelnik
Communications Director
North American Electric Reliability Council
116-390 Village Boulevard
Princeton, New Jersey 08540-5731
Phone: (609)-452-8060
Fax: (609)-452-9550
E-mail: efg@nerc.com

Jose Gracia
Manager, Energy Management
Tennessee Valley Authority
1101 Market Street
Chattanooga, Tennessee 37402-2801
Phone: (423)-751-4923
Fax: (423)-751-4659
E-mail: jrgracia@tva.gov

Herman Green
Project Manager
Alliant Energy
222 W. Washington Ave.
Madison, Wisconsin 53701
Phone: (608)-252-3172
Fax: (608)-252-5551
E-mail: hermangreen@alliant-energy.com

Lou Leffler
Project Manager
North American Electric Reliability Council
116-390 Village Boulevard
Princeton, New Jersey 08540-5731
Phone: (609)-452-8060
Fax: (609)-452-9550
E-mail: lou.leffler@nerc.com

Paula Scalingi
Director, Office of Critical Infrastructure Protection
U. S. Department of Energy
1000 Independence Avenue SW
Washington, DC 20585
Phone: (202)-586-0588
Fax: (202)-586-7221
E-mail: paula.scalingi@hq.doe.gov

Nancy Wong
Critical Infrastructure Assurance Office
U. S. Department of Commerce
1401 Constitution Avenue NW, BM018
Washington DC 20230
Phone: (202)-482-7488
Fax: (202)-482-7498/99
E-mail: nancy.wong@ciao.gov

Craig Zingman
Electrical Engineer
U. S. Department of Energy
1000 Independence Ave., S. W., IJ-051
Washington, DC 20585
Phone: (202)-586-1043
Fax: (202)-586-7221
E-mail: craig.zingman@hq.doe.gov

ATTACHMENTS

ATTACHMENT A: FREQUENCY OF INCIDENTS

Table 1

Transmission Organization "A" (Western U.S. – 17,000 circuit miles) Security Incidents (U)

1998-2000

Frequency	***Incident Type***
24	Vandalism (gunfire damage to power lines, other facilities) other destructive acts
0	Demonstration or protest
4	Sabotage or attempted sabotage (including use of explosive or incendiary devices)
22	Facility break-in/ theft/ attempted theft of materials or equipment
19	Insider crime (mostly petty theft of employee's property)
1	Computer intrusion
29	Miscellaneous
99	**TOTAL INCIDENTS**

Source: Organization "A" Safety and Security Department

Table 2

Transmission Organization "B" (Western U.S. – 15,000 circuit miles) Security Incidents (U)

*1997-2000**

Frequency	***Incident Type***
85	Vandalism/ malicious mischief (including gunfire damage to powerlines)
0	Demonstration or protest
15	Sabotage/ use of explosive device/ bomb threat
181	Break-in/ theft/ vehicle theft/ trespass
50	Insider crime (includes workplace violence or threat of, computer tampering, fraud)
0	Computer intrusion
83	Miscellaneous
414	**TOTAL INCIDENTS**

Source: Organization "B" Security Department; * 10/1/97-4/17/00

ATTACHMENT B: SELECTED PHYSICAL SECURITY INCIDENTS TARGETING U.S. AND CANADIAN INFRASTRUCTURE

INCIDENTS AGAINST U.S. AND CANADIAN INFRASTRUCTURE

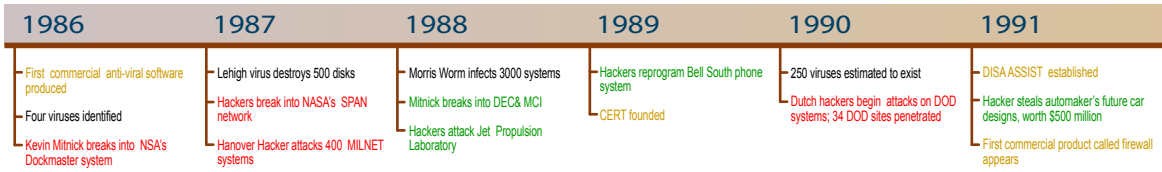
Year	Incident
1973-1978	38 bombings and other attempted violent acts by the New World Liberation Front against PG&E
1982	$12M damage to BCH Cheekye-Dunsmuir substation on Vancouver Island, BC
1989	David Foreman of Earth First convicted of plotting to sabotage the DOE Rocky Flat facility and Palo Alto nuclear power plant
1990	Earth Night Action Group sabotages a 115-KV tower in Santa Cruz County, CA
1997-1998	"Sour Gas" plot – 4 individuals plotted to bomb Texas hydrogen sulfide storage tanks as a diversion for a planned armored car robbery
1998	Vail, Colorado - arson of ski lodge under construction
1999	Ahmad Ressam arrested attempting to smuggle explosives into Washington State from Canada – suspected target Seattle Center
1999	DC tower on BPA HVDC system vandalized in South Central Oregon near Malin
2000	Donald Beauregard, Florida Militia leader convicted of plotting to blow up transmission lines serving the Crystal River Nuclear Plant

ATTACHMENT C: SELECTED DEATHS AND INJURIES FROM FOREIGN AND DOMESTIC TERRORISTS

DEATHS FROM FOREIGN AND DOMESTIC TERRORISTS TARGETING U.S. CITIZENS

Year	Weapon	Incident	Deaths	Injuries
1983	Car bomb	U.S. Marine Barracks, Lebanon	63 killed	
1984	Car bomb	U.S. Embassy, Lebanon	11 killed	
1986	Bomb	La Belle Disco, Germany	2 killed	
1988	Bomb	Pan American flight 103, Lockerbie, Scotland	270 killed	
1993	Van Bomb	World Trade Center, U.S.A.	6 killed	1000 injured
1995	Car Bomb	U.S. Barracks, Saudi Arabia		7 injured
1995	Truck Bomb	Oklahoma City Federal Building, U.S.A.	168 killed	
1996	Truck Bomb	U.S. Barracks, Saudi Arabia	19 killed	
1998	Truck Bomb	U.S. Embassy, Tanzania	11 killed	
1998	Truck Bomb	U.S. Embassy, Kenya	213 killed	5400 injured
2000	Boat bomb	USS Cole, Yemen	17 killed	39 injured

ATTACHMENT D: CYBER INCIDENTS

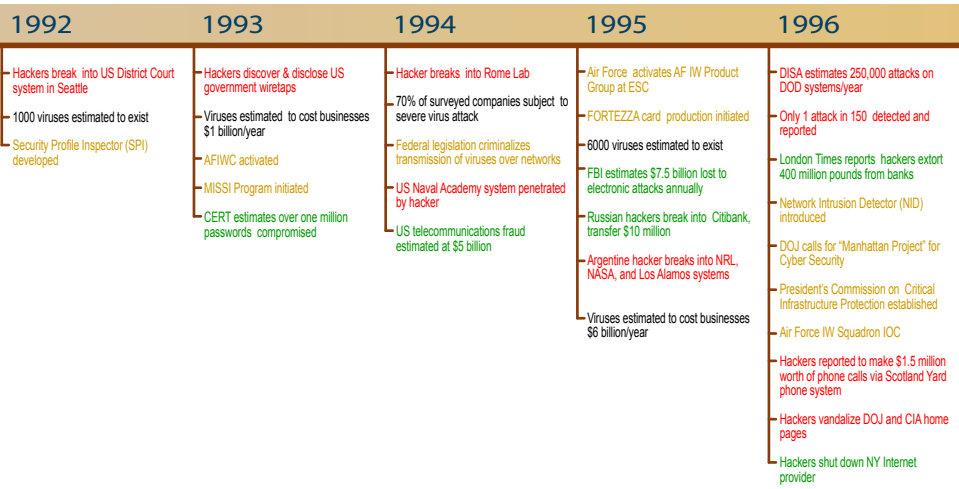


A Chronology of Selected Cyber Events

Color Key:

Attacks on government systems Viruses
Defensive actions Attacks on commercial systems

Compiled by: The MITRE Corporation


1992
Hackers break into US District Court system in Seattle
1000 viruses estimated to exist
Security Profile Inspector (SPI) developed
1993
Hackers discover & disclose US government wiretaps
Viruses estimated to cost businesses $1 billion/year
AFIWC activated
MISSI Program initiated
CERT estimates over one million passwords compromised
1994
Hacker breaks into Rome Lab
70% of surveyed companies subject to severe virus attack
Federal legislation criminalizes transmission of viruses over networks
US Naval Academy system penetrated by hacker
US telecommunications fraud estimated at $5 billion
1995
Air Force activates AF IW Product Group at ESC
FORTEZZA card production initiated
6000 viruses estimated to exist
FBI estimates $7.5 billion lost to electronic attacks annually
Russian hackers break into Citibank, transfer $10 million
Argentine hacker breaks into NRL, NASA, and Los Alamos systems
Viruses estimated to cost businesses $6 billion/year
1996
DISA estimates 250,000 attacks on DOD systems/year
Only 1 attack in 150 detected and reported
London Times reports hackers extort 400 million pounds from banks
Network Intrusion Detector (NID) introduced
DOJ calls for "Manhattan Project" for Cyber Security
President's Commission on Critical Infrastructure Protection established
Air Force IW Squadron IOC
Hackers reported to make $1.5 million worth of phone calls via Scotland Yard phone system
Hackers vandalize DOJ and CIA home pages
Hackers shut down NY Internet provider

1997

- 10,000 viruses estimated to exist
- Hackers make $250,000 worth of phone calls at FBI expense
- NASA & Air Force Web sites vandalized
- Hacker arrested for sniffing 100,000 credit card numbers from Internet
- 50% of surveyed companies suffered electronic intrusion
- Hackers steal computer game source code
- Hacker penetrates and disables Florida 911 system
- 56-bit DES encryption cracked in 210 days
- MasterCard/VISA Secure Electronic Transactions (SET) specification 1.0 published
- Report by Defense Science Board Task Force on Information Warfare released
- Army CERT established
- Computer virus costs Cleveland bank $400,000 in lost operations
- 50% of surveyed companies have been hit with macro virus
- Microsoft, Yahoo, and Value-Jet Web-site all hacked
- Survey indicates that high-visibility electronic commerce web-sites experience 5 serious attacks per month
- 2% of surveyed attacks against electronic commerce web-sites originated from outside the U.S.
- Hacker breaks encryption code used to protect DVD titles
- Hackers suspected of penetrating State Department computers
- Report of President's Commission on Critical Infrastructure Protection released

1998

- Cyber-thieves steal customer data from Sakura Bank
- 20,000 viruses estimated to exist
- Cryptographers crack digital cell phone encryption
- Programmer charged with causing $10 million worth of damage with logic bomb
- Eligible Receiver exercise demonstrates vulnerability of DOD systems
- 64% of surveyed companies suffered computer security breaches in last 12 months
- US Attorney General announces formation of National Infrastructure Protection Center at FBI
- Teenage Hackers penetrate 11 Pentagon Computers
- Hackers claim to have accessed Defense Information Systems Network
- Presidential Decision Directive 63 signed - Critical Information Assurance Office Established
- Hackers breaks into US Coast Guard personnel database
- U.K. hackers deface 500 web sites
- Hackers break into NY TIMES web site
- DoD launches security review of its web sites; temporarily removes data from large number of its public web sites
- 84% of surveyed companies had some form of virus attack in past 12 months
- First internationally coordinated hacker attack detected
- Cyber-thieves hit credit union accounts - nearly $1 million stolen
- 6-bit encryption broken in less than 3 days
- Establishment of Joint Task Force for Computer Network Defense
- GAO Report identifies serious information security weaknesses exist in 24 surveyed agencies
- Hacker attempts to penetrate Russian bank
- Hackers access Indian Nuclear Research Facility

1999

- United States Information Agency hit by hacker
- Hacker attacks force East Timor domain off Web
- Secretary of Defense establishes Joint Web Risk Assessment Cell to monitor and evaluate content of DoD Web sites
- 1999 CSI/FBI survey of corporations indicates for first time that the number of attacks originating from the internet exceed those from internal systems
- Melissa virus, first major e-mail tunneling worm, attacks thousands of computers
- Hundreds of thousands of Asian PCs crippled by Chernobyl virus, first major virus that destroys chips, not just software
- Hackers shut down White House web site
- DoD begins overhaul of its unclassified network to better protect against hacker attacks
- Hackers shut down FBI and US Senate web sites in response to government anti-hacking crackdown
- 1999 Information Security survey reports the average annual corporate loss due to security breaches was $256,000.00
- META/Information Security study indicates that the average corporate security budget rose 21.7% from 1998 to 1999
- Critical Infrastructure Assurance Office proposes 10 point plan cyber-defense plan
- 45,000 viruses estimated to exist
- InformationWeek study shows that computer downtime as a result of security breaches rose 28% from 1998 to 1999
- Serbian hackers attack NATO Web site in retaliation for bombing of Serbia
- FBI reports tens of thousands of US computers had "files infected, damaged or destroyed," by the Worm.Explore.Zip virus, first e-mail tunneling worm that attacks enterprises from behind the firewall
- Cyber skirmishing between China and Taiwan raises international tensions
- Information Security Magazine survey indicates that when companies move operations online the number of intrusions by unauthorized outsiders increases by 24%
- 1999 GAO report indicates that despite some corrective action, serious weaknesses in DOD information security continues to place defense operations at risk
- Hackers compromise security of Hotmail, potentially gaining access to tens of millions of email messages and accounts
- Scientists factor 512-bit encryption key, basis for 95% of keys used for internet electronic commerce
- Viruses estimated to cost organizations $12.1 billion in 1999
- Norwegian hackers crack key to decoding DVD copy protection
- Attack by hacker drives small internet service company out of business
- Financial Services Information Sharing and Analysis Center established

2000

- Hacker posts to a web site 25,000 internet credit card numbers supposedly stolen from CD Universe after failing to extort money from company
- White House releases National Plan for Information Systems Protection, which establishes the first-ever national strategy for protecting the nation's computer networks from deliberate attacks
- Over a three day period hackers, using a denial of service attack, bring down multiple leading web sites including Yahoo!, Amazon.com, eBay and CNN
- According to CSI/FBI survey, 50% of surveyed organizations are using intrusion detection systems, a 19% increase over previous year
- GAO finds that computer security vulnerabilities still exist in the FAA air traffic control systems
- The Common Vulnerabilities and Exposure (CVE) project is recognized for establishing, nurturing and sustaining industry wide cooperation in its effort to establish common naming scheme for system vulnerabilities
- An internet banking service's flawed security policy allowed for $10,000 in illegal transfers
- US Justice Department establishes Computer Crime and Intellectual Property Section (CCIPS) Web site designed to serve as a clearinghouse of cybercrime information and resources
- 70% of surveyed organizations reported unauthorized use of their computer systems within the last 12 months
- ILOVEYOU e-mail virus infects over one million computers worldwide, damage estimated to exceed $4 billion
- Federal CIO Council launches a security best practicies web site
- Flaw in Hotmail allows advertisers to access e-mail acount information of users who click on advertisement banner
- The number of computer viruses now estimated to exceed 50,000
- Hacker breaches Microsoft network, possibly gaining access to unreleased source code
- House panel says federal government cyber security is dismal, gives failing grades to more than a fourth of 24 major federal agencies
- Information Sharing and Analysis Centers established for telecommunications and electrical power industries
- Interpol estimates 30,000 hacker web sites currently exist on the Internet
- First PDA and cell phone viruses identified
- Survey indicates that incidents of employee abuse of computer access controls increased by 11.5% from the previous year
- Department of Justice issues a list of 10 worst Internet security threats and how to eliminate them
- Hacker breaches security at a University hospital, obtains information on 5000 patients
- Hacker breaches Western Union's network and steals nearly 16,000 credit card and account numbers
- US cyberspace chief warns of digital Pearl Harbor
- German Foreign Minister says that cybercrime losses for the G8 have reached over $42.9 billion
- Security flaw allows hackers to steal AOL Instant Messenger screen names and access some users credit card information
- Number of hacker attacks on Pentagon increase by 10% over previous year
- Hacker unsuccessfully attempts to extort money from an online credit card company after stealing 55,000 credit cards from the credit card company

2001

- Information Technology Information Sharing and Analysis Center established
- Security experts estimate that 4 or 5 new viruses are detected each day
- National Intelligence Council report indicates that U.S security threatened by the Internet
- University of California study estimates that hackers cost US businesses 5.7% of annual revenue
- Anna Kournikova virus estimated to have infected millions of computers worldwide
- Hacking by Russian organized crime groups have resulted in more than 1 million stolen credit card numbers
- CSI/FBI survey indicates that 70% percent of those organizations surveyed cited the Internet as a frequent point of attack, an 18% increase over the previous year
- National Security Advisor calls for an "unprecedented" partnership with the private sector to curb the threat of computer-generated attacks on the U.S. infrastructure

ATTACHMENT E: RISK MANAGEMENT APPROACHES

Physical Security

Risk is usually calculated using some variation of the risk equation:

Risk = Probability of Occurrence * (1-Probability of Effectiveness of mitigation) * Consequence

Or:

Risk = Po*(1-Pe)*C

To use this equation, the practitioner must develop the Consequences (e.g., loss of life, loss of revenue, cost of repair, outage time, political damage, etc.). This estimate is converted to a range from *no consequence* to *very high consequence*, and is usually presented in the form of a Consequence Table.

The practitioner must also develop the Probability of Occurrence (or Attack, in ES cases). One of the tools that can be used to develop the Probability of Occurrence is a DBT Table, developed in conjunction with local and national law enforcement intelligence.

Finally, using a Vulnerability Assessment process, the practitioner must find any weaknesses in, and rate the Probability of Effectiveness of, the existing security measures, to establish a baseline.

The risk equation is then used iteratively, in conjunction with other tools, to estimate the cost of a proposed mitigation measure, to determine which mitigation measures are truly effective in reducing the risk, and therefore to determine which proposed mitigation measures are cost-effective.

Cyber Security

The handling of Risk Management for cyber systems is tactically much different, because the effort and the cost are both generally much lower. Typically a Red Team is invited in to run a Security Scanner, War Dialer, Password Cracker, and other attack tools in a controlled attack against the network and the systems on the network. The resulting logs are then examined to develop a list of High, Medium, or Low risk vulnerabilities. Except for the very low-risk items, these typically are fixed from the top down, as quickly as time allows. The Red Team also usually lists some suggestions for strategic improvements; these are often treated as an extension of the tactical list and, again, are all addressed except for the very low-risk items.

ATTACHMENT F: INTERDEPENDENCIES

Historically, the electric industry has been a highly regulated, "natural monopoly" industry. However, in recent years, the generation side has become less regulated and more competitive. Significant changes are taking place as the industry transitions from its traditional, vertically integrated structure to a deregulated structure designed to foster competition. Continuing restructuring is changing the way electricity is produced, priced, traded, and marketed. The electric industry is now made up of traditional electric utilities and "non-utilities," including organizations that consider themselves as cogenerators, small power producers, independent power producers, and exempt wholesale generators. None of these stands alone and independent from its competitors and cohorts. Dependencies include telecommunications, fossil fuels, transportation, banking and finance, water, emergency services, and government services.

Electric Power System: Fuel Dependencies

At the end of 1998, U.S. electric generating capability totaled 775,884 megawatts (MW). Total generation in 1998 amounted to 3,618 billion kilowatt-hours (kWh). The totals for the electric utilities (excluding non-utility power producers) were 687,000 MW installed and 3,212 billion kWh generated. Total generation increased at an annual rate of approximately 2.5 percent per year over the 1993 – 1998 period. Capacity additions planned for 1999 through 2003 total 62,000 MW for nonutilities and only 28,000 MW for electric utilities. This rapid growth by the non-utilities is one example of a restructuring trend.

TABLE D-1: Breakdown of 1998 U.S. Electric Utility Generating Capacity and Generation by Fuel Type

Fuel Type[a]	Total Capacity (%)	Total Generation (%)
Coal	43.7	56.3
Petroleum	5.8	3.4
Natural gas (includes dual-fired)	22.3	9.6
Nuclear power	14.1	21.0
Renewables[b]	0.3	0.2
Hydroelectric[b]	13.8	9.5
Total	**100.0**	**100.0**

[a] Fuel type is classified by primary energy source. Excludes non-utilities. [b] Renewables include geothermal, biomass, wind, solar thermal, and photovoltaic. Hydroelectric is listed separately. Source: DOE/EIA-0629

Coal continues to have the largest share of total utility capacity (44%) and generation (56%), as summarized in Table D-2. Petroleum and gas together account for 28% of capacity, but only 13% of generation: these sources are used more for peaking and daily cycling capacity. However, natural gas is the preferred fuel for most new generating capacity, so its share is expected to grow. Renewables (including hydroelectric) currently represent about 14% of capacity and 10% of total generation.

Including nonutility generation increases the natural gas share of total generation to over 15%. Natural gas is used for 65% of nonutility generation.

TABLE D-2: Breakdown of 1998 U.S. Electric Generation by Fuel Type (includes utility and nonutility)

Fuel Type	Total Generation (%)
Coal	51.7
Petroleum	3.6
Natural gas	15.1
Nuclear power	18.6
Renewables other than hydro	2.0
Hydroelectric	9.0
Total	**100.0**

Total sales to ultimate customers was 3,240 billion kWh in 1998, an increase of 3.2 percent over 1997. Total revenues from those sales were $218 billion in 1998. The average cost was 6.7 cents per kWh. However, regional variations in cost per kWh are large, depending on factors such as fuel location, availability of hydroelectric resources, and historical utility decisions on how to meet growing demand.

Transport of coal to electric power stations is an important dependency of the electric power system. In 1998, over 930 million tons of coal were delivered to electric generators. This accounts for over 90 percent of coal use in the U.S. Coal transport by rail is the most typical delivery, and coal ton-miles account for a large share of all rail shipments.

Natural gas price and availability in recent years caused many dual-fired units (oil and gas) to turn to gas exclusively. Petroleum use for electric generation has been approximately constant at 100 billion kWh per year (about 3 percent of total generation) over the last 10 years. Total generation from petroleum sources is expected to decline in the coming years.

Variations from region to region and state to state are large in the electric sector. For example, Wisconsin's utility generation in 1998 was 76% from coal and 18% from nuclear, with most of the coal was shipped from western states. Oklahoma, as a large natural gas producer, had 60% from coal and 33% from natural gas. New York has a more balanced utility generation picture, with 27% from nuclear, 23% from hydro, 20% from coal, 17% from gas, and 12% from petroleum. Hawaii suffers from the most unbalanced utility generation, with 99.8% from petroleum.

Dependencies of the various states vary according to the location of fuel sources and the available generation sources in the states. Obviously, Hawaii depends heavily on shipments of oil for its electrical generation. Wisconsin depends heavily on rail shipment of coal. Florida's electric utilities use natural gas for only 19% of generation. However, when a major outage of a natural gas pipeline occurred in August 1998, it was the electric sector that had serious problems in the state. Such variations in regional structure affect the level of interdependency and the types of infrastructure assurance measures that need to be considered.

Interdependencies

Infrastructure interdependency refers to the physical, electronic (cyber), and new economy (e-commerce) linkages within and among the critical national infrastructures—energy, telecommunications, banking and finance, electronic commerce, transportation, water systems, emergency services, and government services. These linkages vary significantly in terms of scale and complexity, and typically involve a large number of system components. Identifying and analyzing these linkages requires a detailed understanding of how the components of each infrastructure (e.g., power plants, transmission lines, electric substations, system control centers, natural gas compressor stations, petroleum fuel pipelines, telecommunications end offices, water treatment plants, and traffic control centers) and their associated system functions or activities (e.g., power distribution, natural gas transmission, petroleum fuel distribution, telecommunications switching, drinking water production, and traffic control) depend on, or are supported by, each of the other infrastructures.

The ES, for example, depends on natural gas, coal, and petroleum fuels for their generators; road and railroad transportation to get fuels (other than natural gas and some liquid petroleum products) to the generators; water for cooling and emissions reduction; and, potentially, telecommunications for monitoring system status and system control (i.e., SCADA and Energy Management Systems [EMS]). The electric infrastructure also depends on telecommunications, petroleum fuels (for vehicles and emergency generators), road transportation and, in some cases, railroad transportation, when failures occur and it is necessary to send out repair crews and replacement components.

Similarly, the other critical infrastructures depend on electric power (and the other critical infrastructures) for key functions or activities. For example, natural gas depends on electric power for control systems, storage operations, and some compressor stations; water for injection purposes; and telecommunications for monitoring system status and system control (i.e., SCADA systems). Natural gas also depends on road and railroad transportation, telecommunications, and petroleum fuels for repair and maintenance operations. Likewise, railroad transportation depends on electric power for signaling, crossing protection, monitoring, and certain railroad terminal operations.

Types of Interdependencies

The complexity and interconnected nature of our infrastructures are due largely to an increased reliance on telecommunications and computer processing for their management. The power and sophistication of cyber technologies and their widespread integration in the ES and other infrastructures make unforeseen vulnerabilities and unintended consequences more likely. In addition, not all aspects of one infrastructure's dependence on another are documented or understood. Hidden interdependencies are a strong possibility because of complex and heretofore not-understood linkages.

The most obvious dependencies are physical links. For example, a substation in an electrical distribution system may provide electric power to a telecommunications center. Failure or loss of power in the substation would directly affect the telecommunications center (subject to backup power supplies). The telecommunications center, in turn, may

control the SCADA systems for gas pipelines and water-supply systems. The gas pipelines may fuel critical gas-fired generators in the electric system, and so forth. Such dependencies are often called *first-order system interactions*.

Other dependencies are not physically linked but are coupled because of location and exposed environment. For example, a common utility corridor may contain overhead electric power transmission lines, buried gas pipelines, and telecommunications cables. Collocating infrastructures makes them more susceptible to such physical hazards as explosion, fire, flood, and seismic events, as well as sabotage.

Subtle interactions are another type of dependency that can exist in complex systems and occur without a direct link. The failure of a substation, for example, could cause topological reconfiguration of the electric network. Reconfiguration could then overload a similar substation within the system if the demand at that time exceeded the substation capacity. Here, the direct link does not normally exist, and the failure could occur only if certain conditions were imposed (e.g., peak load).

Direct system interactions, indirect coupling as a result of collocation, and subtle interactions usually occur shortly after an incident. However, another type of interaction can occur over an extended time, as the effect propagates through elements of the infrastructures. Understanding this time delay is important in designing appropriate detection and mitigation technologies. Infrastructures such as the water-supply system and gas and oil storage that are limited resources subject to depletion are candidates for these interactions. Also, the effect of threats (e.g., cyber threats to the banking and finance infrastructure) requires time to propagate: early detection and recovery are important factors in controlling their effects.

Natural hazards, such as seismic events or extreme weather, clearly illustrate how threats can affect multiple infrastructures simultaneously. Such threats also reveal interdependencies that can complicate or delay mitigation or recovery of a particular infrastructure from an incident. A major earthquake, for example, can disrupt many infrastructures. At the same time, transportation structures, such as bridges and elevated highways, could collapse, making it difficult to provide vital emergency services.

Consequences of multiple disruptions to our infrastructure range from loss of human life and property to prolonged loss of shelter, food, and water, and disruption of financial services. Recovery of particular infrastructures from an incident can be delayed significantly or thwarted by the simultaneous unavailability of the ES and other infrastructures. Controlling or reducing the effect of interdependencies is a function of the type of incident, the area of occurrence, and the technology.

Electric Power Interdependencies with Other Infrastructures

The ES infrastructure is centrally important for operating other critical infrastructures. Each infrastructure depends to varying degrees on electric power for systems and facilities, as well as emergency backup power. For example, power outages affect virtually every mode of transportation, including subways, elevators, and street traffic (no traffic lights or gasoline pumps).

On the other hand, the ES infrastructure depends strongly on the oil and gas delivery and storage infrastructure and on the transportation infrastructure for delivery of fuel, including coal, which supplies more than half of all electric generation. The ES infrastructure also depends to varying degrees on the telecommunications infrastructure for vital communications. The ES infrastructure also depends on other critical infrastructures to varying degrees for financial services and transactions, for water supply, and for emergency and government services.

A few examples of important dependencies are listed here.

Telecommunications are affected by extended power outages. The extent of the disruption depends on whether telecommunications networks, both public and private, have emergency backup power systems and how reliable the backup systems are. The importance of backup power systems was shown during the 1989 Hurricane Hugo and San Francisco earthquake outages. At the height of Hurricane Hugo, 39 central offices and 450 digital loop carrier facilities were operating on backup power. Southern Bell indicated that the facilities could operate on battery power for about 8 to 10 hours before gas or diesel generators took over. With the commercial power turned off in San Francisco because of the risk of fire, central offices operated on diesel generators. These diesel generators could operate for up to 7 days.

The ES infrastructure depends on telecommunications systems in many ways, e.g., for monitoring performance and changing operating levels of generation, transmission, and distribution systems and for security systems.

Oil and gas systems require electric power in virtually all aspects of the industry, including production, processing, transmission, storage, distribution, and marketing and business functions. The importance of a reliable supply of electric power is reflected in the widespread use of emergency generators at critical facilities in the industry, although emergency generators typically are intended to keep essential functions operational, not to provide sufficient power to keep full-scale operations underway. The impact of a power outage is magnified because both shutdown and start-up are phased. An 8-hour power outage in a refinery may lead to a 40- to 60-hour shutdown.

The electric industry depends on oil and gas for about 13% of total generation by electric utilities (1998). Traditionally, this generation typically occurs at or near peak load times, so the contribution is very important. Also, as natural gas is the preferred fuel for new generating capacity, it is rapidly becoming a larger and more important contributor to electrical generation.

Transportation systems, including airlines, subways, traffic control, trains, elevators, gas stations, and many others, are severely affected by electrical blackouts. For example, airports are powered by auxiliary generators that enable aircraft to land and take off in an emergency, but usually with considerable delays

The ES infrastructure depends on transportation systems for delivery of fuel (rail, truck, barge, pipelines, and ships), for delivery of equipment and components, and for safe and timely arrival and departure of operating and construction staff. Transport of coal is one of the largest activities of the nation's railroads.

Banking and finance depends on reliable electric power for operation of automatic teller machines, computers, offices, and security equipment. Electronic commerce is normal operation in the banking industry; it is also critical for the electric industry itself. The financial structure (debt-equity) of the electric industry and recent innovations, such as power marketing, critically depends on the banking and finance industry. In the capital-intensive electric industry, with long payback periods and low operating margins, the availability of capital is critical for investment decisions.

Electronic Commerce depends on reliable electric power to run the servers and telecommunications circuits that, taken together, form the Internet and the other electronic commerce systems. At the same time, the new business environment in which the ES must operate is critically dependent upon automation and electronic commerce. Futures markets, real-time data exchange, electronic transactions, and just-in-time delivery are the hallmarks of this new environment. The global electronic systems that make this environment possible transcend traditional physical boundaries. They have created new vulnerabilities and a marked increase in the interdependence of the participating entities. Disruptions of the electronic marketplace could result in potential loss of service, loss of stakeholder confidence, and/or the failure of ES organizations.

Water supply systems depend on electricity for operations, such as pumping and metering. The electric industry critically depends on water for cooling generating plants. The rejection of waste heat in the generation process requires access to major water sources and results in significant evaporation.

Emergency services include police and fire and their communications and transport, as well as hospitals. Power outages also affect these services. Hospitals generally have emergency power systems to support the most critical activities, but not others. Fire-fighting and police communications can be severely disrupted by the loss of power. Fire alarm systems may be inoperable, and water pumping may be hampered. Moreover, the indirect impacts of a blackout, such as looting and arson, can severely strain fire-fighting and police services.

Government services depend on reliable electricity for continuity of operations.

The ES depends on government services for permitting, regulatory authority, and a structure under which successful business can be practiced.

Interdependence-related Disruptions

Interdependence-related infrastructure disruptions or outages can be classified as cascading, escalating, and common cause.

- **Cascading Failure.** A disruption in one infrastructure causes the failure of a component in a second infrastructure and the subsequent disruption in that second infrastructure. For example, the disruption of a distribution network within the natural gas infrastructure that has an electric utility's generating unit in its service territory may result in a failure (disruption) of that generator, which in turn could lead to a shortage of generation in the area and thus potential power disruptions (a cascading failure from the natural gas infrastructure to the electric infrastructure).

- **Escalating Failure**. An existing disruption in one infrastructure exacerbates an independent disruption of a second infrastructure, generally in the form of increasing the time for recovery or restoration. For example, a disruption in a telecommunications network (e.g., a failure of an end office) may be escalated by a simultaneous or subsequent disruption of a road transportation network that would delay the arrival of repair crews and replacement equipment.

- **Common Cause Failure**. Two or more infrastructure networks are disrupted at the same time because components of each network fail as the result of a common cause. The common cause may affect components from multiple infrastructure networks either because the components occupy the same physical space (e.g., a right-of-way corridor) or because the cause is widespread (e.g., a natural disaster, such as an earthquake or flood, or a human-caused disaster, such as a terrorist act). For example, telecommunications cables (both wire and fiber) and electric power lines often follow railroad right-of-ways. Consequently, an earthquake that severs railroad tracks could also disrupt communications cables and power lines that are located within the same corridor.

A well-organized, coordinated sabotage event could cause a wide-area disruption of one or more infrastructures. A series of incidents, each planned and timed to reinforce the effects of the others, could interact (cascade) across critical infrastructures to degrade the services upon which all depend. The finely tuned, just-in-time interdependence of infrastructure systems gives potential attackers the capability to leverage localized damage into widespread system failure. A lesser sabotage could also propagate across several infrastructures where embedded dependencies exist within the architectures of our infrastructures.

Actions to Address Interdependencies

The ES needs to develop a greater awareness of critical infrastructure protection issues, not only within the sector, but more broadly from an interdependencies perspective. If power system planners and operators fail to understand how disruptions to one infrastructure could propagate throughout the infrastructures, they will not be prepared to deal effectively with multiple infrastructure contingencies. In the highly interconnected economy of the future, hostile—and non-hostile—disruptions will have much greater ability to reverberate throughout the infrastructures, including the ES, unless "shock absorbers and circuit breakers" are built in to prevent it.

The greatest challenge is to identify and fully understand the linkages among the infrastructures (i.e., the interdependencies) and what they mean. While tools exist that allow us to model single infrastructures (such as the electric power grid), models and simulation tools for multiple, coupled infrastructures, and the requisite network databases, are rudimentary at best. Even the capability to draw general conclusions about the behaviors and properties arising from interdependent effects is very limited.

Greater awareness, coordination among the nation's infrastructure service providers and with government, and research are needed to address these issues. The research must be conducted from a holistic perspective to capture the "system-of-interacting-systems" nature of our critical infrastructures: its complex behaviors, its vulnerabilities, its robustness and whether it degrades gracefully when stressed, the effects of its interconnections with other infrastructures, and its interfaces with human operators and users. **Interdependencies workshops and exercises need to be held to facilitate awareness and the development of an integrated interdependencies strategy that will lead to cost-effective avoidance, assurance, detection, and recovery actions.**

ATTACHMENT G: SAMPLE CRITICAL ASSET IDENTIFICATION LIST

Physical Assets

National Security

Will the loss or compromise of the electrical infrastructure asset disrupt or otherwise threaten the ability of the United States, Canadian or Mexican military or civil government to satisfy their critical mission in support of national military or civil security?

A few examples might include electrical infrastructure that supports the following:

- critical military bases,
- intelligence functions,
- emergency management facilities,
- satellite communications facilities,
- critical government offices, and
- critical military weapons manufacturers.

Public Health and Safety

Will the loss or compromise of the electrical infrastructure asset disrupt or otherwise threaten the public safety and health, and/or environment of the United States, Canada or Mexico?

A few examples might include electrical infrastructure that supports the following:

- potable water supplies,
- sewage treatment facilities,
- critical traffic signals,
- critical fire and police facilities,
- street lights in critical areas,
- communications facilities, and
- hurricane tracking centers.

Economic Security

Will the loss or compromise of the electrical infrastructure asset disrupt or otherwise threaten the economic security of the United States, Canadian or Mexican economy?

A few examples might include electrical infrastructure that supports the following:

- critical banking facilities,
- critical electronics industries,

- petroleum refineries, and
- petroleum and natural gas distribution facilities.

Regional and National Electrical Grid Reliability

Will the loss or compromise of the electrical infrastructure asset disrupt or otherwise threaten the regional, national, or North American electrical grid reliability?

A few examples might include electrical infrastructure such as the following:

- important regional transmission hubs,
- interregional tie lines,
- substations that feed interregional ties,
- interregional communications facilities, and
- security centers.

Generation

Will the loss or compromise of the electrical infrastructure asset disrupt or otherwise threaten the supply of generation necessary to adequately serve the regional, national, or North American electric demand?

A few examples might include electrical infrastructure such as the following:

- major generation facilities,
- substations that integrate major generation into the grid,
- transmission lines that link major generation to the grid, and
- any facilities necessary for nuclear power plants.

Cyber Assets

Any list of critical cyber assets will vary from organization to organization within the ES, depending on the nature of the enterprise. Power marketing entities will have a much different list of cyber assets than will a high-voltage transmission organization. One possible criterion (which may not be appropriate for all ES members) is shown below. Using this criterion, a power marketer might not have any systems designated as critical. That may be appropriate, since loss or degradation of its cyber systems may not have much effect on the electric grid. That does not mean that their systems are not important: in fact, the survival of the organization could depend on them. Loss or degradation of their cyber systems could also erode public confidence in the ES. Even so-called "non-critical" systems require a relatively high level of protection, if for no other reason than that they may share the same network with more critical systems, with only a firewall in between.

Critical Control Systems

Will the loss or compromise of operational systems disrupt or otherwise threaten control of the generation, transmission or distribution of electricity in real time?

A few examples, for the case of a high-voltage transmission organization, might be the following:

- Supervisory Control and Data Acquisition (SCADA) Systems,
- Automatic Generation Control (AGC) Systems, and
- Generic Data Acquisition and Control System (GDACS).

Essential Business Systems

Will the loss or compromise of operational systems disrupt or otherwise threaten operational reliability and business systems that could have a significant impact on financial operations?

A few examples, for the case of a high-voltage transmission organization, might be as follows:

- Outage Scheduling Systems,
- Network Domain Controllers, and
- Firewalls.

Non-critical Systems

All remaining systems. A few examples, for the case of a high-voltage transmission organization, might be as follows:

- Open Access Same Time Information Systems (OASIS) Reservations Systems,
- E-tagging Systems,
- Dispatcher Training Facility (DTF) Systems,
- Lightning Monitoring Systems, and
- Power and Transmission Scheduling systems.

ATTACHMENT H: FACTORS TO CONSIDER IN SELECTING PHYSICAL AND CYBER SECURITY VA TOOLS AND METHODOLOGIES

Physical security can be divided into "tactical" and "strategic" parts. Many physical security programs focus on tactical concerns. It is extremely important to include strategic considerations when selecting a physical security methodology.

Tactical

- Security Policy – Does the enterprise have a written physical security policy? Are the processes in place to keep it up to date? Are the processes in place to keep all employees aware of the security policies on an ongoing basis? Are the policies enforced?
- Managing Access – Does the enterprise manage the keys or card keys used for access? Are they collected when employees retire, resign or are released? Are access codes changed on a regular basis, and whenever an employee is terminated?
- Fences – Are fences installed around all critical facilities? Is the first access control located out at the fence?
- Intrusion Detection – Are intrusion detection sensors installed on all critical facilities? Are the sensors maintained and monitored? Do the sensors have a high rate of false alarms leading, monitoring staff to ignore alarms? Are sensors installed in layers to raise the probability of detection?
- Security Systems – Are security systems installed in high-traffic critical facilities? Are the access lists kept up to date, with employee access removed when they retire, resign, or are released?
- Training of Physical Security Staff – Does the enterprise have a training program in place to train physical security staff?
- Insider Treat – Does the enterprise run background checks on prospective and existing employees?
- Shredding – Does the enterprise consistently shred drawings and other documents that could contain security-related and business-sensitive information?
- Emergency Plans – Does the enterprise have emergency response plans, communications plans, and other plans and processes in place to move quickly in case of attack or natural disaster? Are the processes in place to keep employees aware of the emergency procedures? Do the processes include protecting evidence for possible prosecution?

Strategic

- Long-range Planning – Does the enterprise include physical security in its long-range plans, such that security is built into the design of new

facilities from the beginning? Also, is physical security given the same level of consideration as other business needs?

- Intelligence Gathering – Does the enterprise have the processes and protocols in place to exchange information with other local and national law enforcement organizations to monitor possible threats as they develop? Are the physical security systems and processes adaptable and able to respond to changes in the Design Basis Threat (DBT)? Also does the enterprise consider physical security concerns in the information that they post on signs, in what they distribute through their public affairs office, and in what they post on the Internet?
- High Reliability Architecture – Does the enterprise employ a design for their communications systems, control centers, and electrical transmission systems that uses redundancy, alternate routing, and other features to assure high reliability?
- Response – Does the enterprise have the necessary processes and protocols in place to assure as quick and effective a response by local and national law enforcement agencies and fire departments as is possible, given the distributed nature of electrical facilities? Do they run cooperative drills to familiarize law enforcement and fire departments with their facilities?
- Management Support for Security – Does the management of the enterprise wholeheartedly support security? Do they support adequate funding for security? Do they encourage employee adherence to security policy and do they exhibit good security practices themselves?

Factors to Consider in Selecting Cyber Security VA Tools and Methodologies

A strong cyber security posture can be divided into two parts. The first is to have good "tactical" cyber security practices in place; the second is to have strong "strategic" cyber security processes. Most existing cyber security methodologies, such as "Red Teaming"[5] deal almost exclusively with tactical issues. When choosing a cyber security methodology, it is extremely important to include the strategic issues.

Tactical

- Password Management – Does the enterprise have the tools and processes in place to assure that weak or non-existent passwords are quickly detected and corrected, and to assure that employees do not continue to violate password management policy?
- Configuration Management – Does the enterprise have the tools and processes in place to assure that the configuration of computer systems is managed with security in mind? It should encompass the whole

[5] A "red team" is a team of cyber security specialists invited in to attack cyber systems to test cyber security without causing damage

process from Development, through Testing, to Operational status. This should include documenting the need for changes (change management), design walkthroughs, code walkthroughs, controlled builds, source code management, controlled test environments, regular version releases, and a process for backing out changes if errors still creep in.

- Managing Privileges – Does the enterprise have processes in place to assign only the minimum necessary privileges for employees to do their jobs?
- Managing Modems – Does the enterprise have processes in place to assure that modems and analog phone lines are managed? Are modems set up as "output only" wherever possible; and, where not possible, is dialback, or some other more secure mechanism used?
- Security Policy – Does the enterprise have a security policy; is it written down and are the processes in place to keep it up to date? Are processes in place to keep employees aware of the security policies, not just new hires, but all employees on an on-going basis?
- Unneeded Services – Does the enterprise turn off all unused services on firewalls, networks, and servers and only enable those services minimally necessary to conduct business?
- Network Scanning – Does the enterprise have tools and processes in place to scan their own network for vulnerabilities on a regular, frequent basis? Are the vulnerability metrics tracked and trended and is the trend decreasing?
- Intrusion Detection – Does the enterprise have effective intrusion detection tools and processes in place? Does the process take effective action against intruders and are intrusion attempt metrics tracked?
- Software and Firmware Versions – Does the enterprise have a process in place to keep software and firmware up to date with the latest vendor patches for known vulnerabilities?
- Firewall Holes – Does the enterprise have a process in place to assure that holes are not opened through the firewalls for purposes such as importing data files?
- Training of Cyber Security Staff – Does the enterprise have a training program in place to train cyber security staff in the latest techniques necessary to keep up with the state of the art?
- Insider Threat – Does the enterprise conduct background checks on existing and prospective Information Technology (IT) staff and particularly on cyber security employees?
- VERT/CERT – Does the enterprise have Virus Emergency Response Teams (VERT) and/or Cyber Emergency response Teams (CERT) in place for incident handling and does the enterprise have

communications plans and other processes in place to move quickly and effectively in case of attack? Do these processes include saving logs for possible prosecution?

- Self-Assessments – Does the enterprise conduct regularly scheduled self-assessments of the state of their cyber security program?
- Independent Outside Assessments – Does the enterprise have a process in place to conduct regularly scheduled independent outside assessments of the state of their cyber security program?
- Internal Communications – Does the enterprise have the processes in place to effectively share information on new patches, emerging threats and vulnerabilities, new techniques, etc.?

Strategic

- Long-range Planning – Does the enterprise include information and cyber security in its long-range plans, such that security is built into information system design from the beginning? Also, is cyber security given the same level of consideration as other business needs from both a funding and a functionality viewpoint?
- External Connections – Does the enterprise demand the same concern for security from the entities with which they maintain external dedicated connections as they do for their own internal security?
- Intelligence Gathering – Does the enterprise have the tools and processes in place to keep abreast of developments in the hacker community and to keep an eye on any information about themselves posted on the Internet?
- High Availability Architecture – Does the enterprise employ a design for their Energy Management Systems (EMS) that uses redundant systems, automatic failover, and other features to assure high availability?
- Management Support for Security – Does the management of the enterprise wholeheartedly support security? Do they support adequate funding for security? Do they encourage employee adherence to security policy and do they exhibit good security practices themselves?

ATTACHMENT I: GENERIC THREAT SPECTRUM

Draft Generic Threat Spectrum - Sample for Discussion Only

Threat Spectrum

Physical Domain — **Cyber Domain**

Category	Definition	Threat/ No-Threat	Category	Definition	Threat/No-Threat
Vandal	Small group -rifle, handgun, hand tools	Unlikely to cause widespread grid problems (e.g., DC tower)	**Hacker**	Small group - PCs, InterNet, phone, E-mail viruses, DDoS, HTML, etc.	Presents very little threat to EMS systems and is extremely unlikely to cause any problems to the electrical grid. They do, however, present a possible threat to the E-business systems.
Psychotic	Loner	Unlikely to cause widespread grid problems	**Cracker**	Small groups - PCs, phones, war dialers, password crackers, etc	Some EMS systems could possibly be exploited by crackers. Any effects would probably be uncoordinated and are unlikely to cause widespread problems for the electrical grid.
Extortionist	Small groups - pipe bombs, small bombs	Unlikely to cause widespread grid problems (e.g., Jay Hawker)	**Industrial Espionage**	Small group - PC's, Internet, "dumpster diving"- Looking for information but unwilling to take any significant risks.	Extremely unlikely to cause any problems for the electrical grid. Have the potential to cause economic damage.
"Postal" Employee	Loner-handgun, rifle, automatic rifle	Unlikely to cause wide-spread grid problems; possible hostage situations-e.g., Hawaii	**Organized Crime**	Small group	Extremely unlikely to cause any problems for the electrical grid.

Category	Definition	Threat/ No-Threat	Category	Definition	Threat/No-Threat
Disgruntled Employee	Small group - may know what is really important	Could cause widespread grid problems - could be recruited by sub-national/ ultra-nationalist/ eco-terrorists	**Disgruntled Employee**	Small group - May know what is really important.	May be able to cause major problems for the regional electric grid, even working alone. Could be recruited by eco-terrorists, terrorists, or nation states and thus, maybe even unwittingly, be used to cause wider outages.
Eco-Terrorist	Small groups - could target existing dams or new lines/ substations built in ecologically sensitive areas	Unlikely to cause widespread grid problems - e.g., Vail	**Eco-Terrorist**	Small groups - PCs, Internet, phones - Could target government or big business that damages the environment, or to right perceived wrongs. Could deface web sites or take other highly visible and embarrassing actions.	Unlikely to cause widespread problems for the electrical grid.
Survivalists/ Ultra-Nationalists	Small groups- truck bombs, hand guns, rifles, automatic rifles- could target government facilities	Unlikely to cause widespread grid problems. Could seek major casualties- e.g., Oklahoma City	**Terrorists**	small groups - PCs, Internet, phones, DoS, DDoS - looking to have a major impact on the infrastructure with the goal of harming the U.S. economy or damaging U.S. confidence. Have the time and resources to conduct careful probing to determine the most effective targets and to conduct coordinated attacks.	Capable of causing great harm to the E-business infrastructure but unlikely to cause widespread grid problems through cyber attacks. Could be recruited by nation-states.
Sub-National Terrorists	Small groups - truck bombs, handguns, rifles, automatic rifles - seeking large	Capable of causing great disruption to the electric grid. Willing to take risks or die in the attempt - e.g., U.S. Embassies; Africa	**Nation-States (Information Warfare)**	Information Warfare - Mainframes, PCs, InterNet, phones, DdoS, HTML, E-mail viruses, war dialers, password crackers, scanning tools and	High probability that they could crash some EMS systems (DoS) but, unless the crashes are accompanied by coordinated physical attacks on the grid, they

Category	Definition	Threat/ No-Threat	Category	Definition	Threat/No-Threat
	number of casualties or major impact on infrastructure.			other sophisticated tools - Looking to cause long term problems that would adversely affect the U.S. economy and U.S. ability to wage war. Have the time/resources to conduct careful analysis and pick effective targets to conduct coordinated attacks.	are unlikely to cause major disturbances to the electrical system. High probability that they could have serious long term effects on E-business systems (DoS, DDoS or HTML attacks) causing serious financial loses and seriously damaging U.S. confidence.

ATTACHMENT J: COOPERATIVE GOVERNMENTAL PROGRAMS: INDICATIONS, ANALYSIS AND WARNING (IAW)

Background

The Department of Justice and the Federal Bureau of Investigation (FBI) established the National Infrastructure Protection Center (NIPC) at FBI Headquarters in Washington, D.C. NIPC is a joint government and private sector partnership that includes representatives from the relevant agencies of federal, state, and local government, and from the private sector. The NIPC serves as the national focal point—a fusion center—for threat assessment, warning, investigation, and response to attacks on the critical infrastructures. A significant part of its mission is to establish mechanisms to increase the sharing of vulnerability and threat information between the government and private industry.

It is fitting and no accident that NIPC's first IAW initiative focuses on electric power. Recently, the National Academy of Engineering ranked the 20 greatest engineering achievements of the last century. On the basis of its effect on the quality of life, electrification, or electric power, was rated first.[6]

With the assistance of government officials and ES industry representatives, the NIPC developed general guidelines for voluntarily reporting any operational and cyber incidents adversely affecting the nation's electric power infrastructure; i.e., a prototype NIPC IAW initiative for the electric industry. The NIPC IAW initiative has two goals:

1. tactical—to warn of impending attacks or likely developments during the early stages of an attack; and,
2. strategic—to warn of longer-term threats to and vulnerabilities in critical infrastructures.

The Initiative: An Overview

In its Electric Power IAW program, the NIPC seeks timely reports from industry on incidents meeting one or more of 15 predefined event criteria. Cyber attacks and threats, physical attacks and threats, and combinations thereof fall within the range of activities of malicious origin, or unknown and potentially malicious origin, for which this IAW system is developed.

Operating personnel stationed in power system control centers are responsible for initiating the reports. These centers are manned around the clock (7x24) and are responsible for keeping power systems in balance (i.e., generation = load) at all times. Intra-organization communications discipline is essential within the business enterprise to assure that all relevant personnel (i.e., physical security, IT security, and operations) are kept aware of incidents reported to and warnings received from the NIPC.

The IAW program has a three-stage cycle for incident reporting:

[6] Report of the U.S. Department of Energy's Power Outage Study Team, March 2000, pg. S-1.

- Stage 1—within 60 minutes of incident detection;
- Stage 2—within 4-6 hours of the Stage 1 report; and,
- Stage 3—whenever the reporting entity assembles enough information to close out the incident, nominally within 60 days.

Communications

Incident Reporting by Industry. To secure the broadest participation in the IAW program, the standard Incident Reporting Format (which features a document template) resides on and can be used to report incidents through the FBI's secure InfraGard web-server. Once filed, the report will return to the originator a unique identification number for that particular filing. The Incident Reporting Form also contains data fields (Section I) that may be set up to reflect pre-established profiles for ease of filing. For confidentiality and proprietary reasons, these fields will not be divulged by the NIPC in any warning notices that may be issued, but will be further disseminated to NERC.

Additionally, incident reports can be sent by the originator to the NIPC Watch & Warning Unit using the email or FAX addresses shown on the reporting form.

NIPC Warning Products. Some information available to the NIPC may be classified or law-enforcement-sensitive and, thus, unavailable to many in the industry. A select group of NERC officials and other designated industry personnel is being sponsored for clearances by, and at the expense of, the NIPC and will be provided with the means to access classified material. This group will advise the NIPC on matters of declassifying and sanitizing warning material so that it may be disseminated to all appropriate personnel industry-wide. Once the NIPC has determined that a warning should be issued, all or a sufficient subset of these advisors will be available as needed to assist the NIPC in sanitizing and finalizing warning notices so as to provide non-proprietary, timely and *actionable* information to the maximum extent possible.

Table 4 (following page) describes the plan envisioned by this SOP for disseminating warning products.

Table 4: Proposed Dissemination of Warning Products

Class of Information:	Distribution Media:	Recipients:
Classified	-STU-3 -Secure FAX -Secure teletype	Participating industry and government personnel with appropriate clearances and need-to-know for each particular incident.
Limited Distribution ? InfraGard "Secure Information" ? Other information in accordance with submitter's restrictions	 Secure InfraGard web server and email Email or fax via NERC	 InfraGard Members with signed Agreement Electric Power entities
Public	NIPC public web server NIPC email to NERC	All NERC and electric power entities

Information to be Shared

A standardized format for reporting all three stages of incident data has been developed; up-to-date copies will be maintained on the secure NERC (to be supplied) web-site. At each subsequent stage, as defined below, it is anticipated that personnel submitting incident reports will be able to provide more complete and definitive information until, at Stage 3, the incident is effectively closed out. At any time, originators may terminate reporting on any incident determined to lack malicious intent by so changing the entry in block #7 (Cause of Outage/ Degraded Operation), Section 1 of the Incident Report Form, and sending a revised report to the NIPC.

NERC Outreach

The IAW program is implemented under two separate time frames: initial and sustaining. Initially, NERC intends to sponsor regional workshops open to power sector entities interested in participating in the information-sharing program. Each workshop will provide stand-alone instruction, guidance, and materials, so that participants can set up program operations at their facility. Four workshops are planned: one in the Western Systems Coordinating Council; one in the Electric Reliability Council of Texas; and two in the Eastern Interconnection.

Separately, and to sustain the indications and warning program over the longer term, NERC intends to add essential elements of NIPC's IAW program to its operator training and recertification syllabus.

On July 12, 2000, the NERC Operating Committee approved the voluntary reporting through the Electric Power IAW by Control Areas, Security Coordinators, and NERC member organizations in North America.

ATTACHMENT K: CRITICAL INFRASTRUCTURE PROTECTION AND INTERNET SECURITY

Major Governmental Activity
Year 2000

Summary

Some current progress, but primarily sets the stage for further action next year.

Legislation Signed

Department of Defense Authorization Act (Pub. Law 106-398) — "Bennett-Schumer" Amendment

DoD is:

- required to better define its role in, and explain to Congress its coordination with, other governmental efforts related to, critical infrastructure and information system protection
- given $15 million to recruit cyberwarfare specialists
- given $5 million to create an Institute for Defense Computer Security and Information Protection
- authorized to provide loan guarantees to improve domestic preparedness to combat cyberterrorism

Requires the President to:

- coordinate federal infrastructure protection efforts
- report to Congress on progress by DoD and all other agencies in developing information security plans for both private and public sectors

Legislation Vetoed

Department of Justice Appropriations (part of H.R. 4690) — attached to D.C. spending bill (H.R. 4942)

Although this measure is expected to be vetoed due to the scope of its immigration provisions, DoJ would get over $204 million to implement the Communications Assistance for Law Enforcement Act (CALEA), bringing the total up to the $500 million needed for full implementation. The FBI would get over $17 million for CALEA, but was ordered to reorganize its CALEA and other electronic surveillance activities. Among other related Internet and technology funding, DoJ would also get $25 million for the FBI's "Digital Storm," $5 million for the Counter Terrorism Fund, almost $4 million for the Cybercrime and Intellectual Property Division, and $2 million for the FBI's Joint Terrorism Task Forces.

House Bills

H.R. 2413 — Computer Security Enhancement Act of 2000
passed by House

H.R. 2413 would require the National Institute of Science and Technology (NIST) to serve as a computer security consultant for federal civilian agencies. NIST would offer the government guidance on protecting the security and privacy of sensitive information in agency computer systems. In this role, NIST would be encouraged to recommend "technology neutral" solutions to security problems, and to advise government agencies on which "off-the-shelf" computer security products met with the government's standards. H.R. 2413 also would require NIST to study the effectiveness of commercially available encryption products. The results of that study would be made available to federal agencies and to the public. Also to be made available to the public would be a clearinghouse of information on computer security threats to be created by the Under Secretary of Commerce.

H.R. 4246 — Cyber Security Information Act
Davis, Moran, Cunningham, Rogan
referred to Judiciary and Government Reform (hearing 6/22/00) Committees

H.R. 4246 accomplishes two major goals. First, it provides limited protection from unintended uses for cyber-security information voluntarily shared with the federal government. Second, it describes alternative mechanisms for sharing such information with the government. A bill with a similar information-sharing provision has recently been introduced in the Senate (S. 3188, below).

As for the mechanisms for sharing cyber-security information with the government, the Act specifies that the government may ask for voluntary submittal, directly to the government, of detailed organization-specific cyber-security information (as defined) in order to assess the cyber-security of an industry or economic sector. Further, the government may request that cyber-security data be submitted to a non-governmental entity that agrees to coordinate such data-gathering and then pass on that information to the government, most likely by means of its own summary and assessment of the data. In addition, such non-governmental entity may obtain the benefits of this provision even if it performs those functions without first being asked by the government, as long as it does in fact provide such cyber-security data and/or analysis to the government.

Next, regarding the protections provided to cyber-security information, the Act stipulates that any and all cyber-security information (as defined) voluntarily provided to the government or aforesaid non-governmental entity will be given a broad immunity from forced release to any other entity or individual. This is accomplished in two ways. First, the Act specifies that all cyber-security information voluntarily provided to the government pursuant to this process is deemed to be exempted from disclosure under the Freedom of Information Act (FOIA). This exemption is similar to already existing FOIA exemptions, such as

those for trade secrets and national security, but would not be subject to the uncertainties, vagaries, and delay of case-by-case agency determination, along with any attendant litigation delays associated with making such case-by-case determinations. Moreover, to the extent that any such cyber-security data actually held by a third party could be said to be held by the government by virtue of that third party acting on behalf of the government, FOIA would still not require the release of such data.

Second, no entity may use any other means (such as a subpoena) to force the government or the third-party data-gatherer to yield up cyber-security data. However, to ensure that the government obtains the full use of any related or similar data that it receives, and that no injustice would be worked against a party to litigation, the Act further provides that cyber-security data can be used **(a)** by the government if obtained pursuant to some statutory or regulatory requirement (rather than voluntarily), or **(b)** by anyone for any purpose once the information has been made public with the permission of the originating entity. Moreover, a litigant may utilize any existing lawful means already available to it (such as a subpoena) to obtain such data directly from the originator.

H.R. 4987 — Digital Privacy Act of 2000
Barr, Emerson
referred to Judiciary Committee; Constitution Subcommittee held hearing 9/6/00

Would ease law-enforcement monitoring of electronic communications.

H.R. 5018 — Electronic Communications Privacy Act of 2000
Canady, Hutchinson, Blunt, Bachus, Paul, Wamp
was scheduled for House vote

As substantially revised, H.R. 5018 is primarily focused on privacy concerns raised in reaction to the FBI's "Carnivore" e-mail surveillance program. Because it is vastly different from the primary Senate-passed cybercrime bill (S. 2448, below), no further action is likely at this late date in the legislative year.

Senate Bills

S. 1314 — Computer Crime Enforcement Act
Leahy, DeWine, Robb, Abraham, Hatch
was scheduled for Senate vote

S. 1314 would authorize $25 million for DoJ to help states develop computer crime enforcement units.

S. 1993 — Government Information Security Act
Thompson, Lieberman, Abraham, Voinovich, Akaka, Cleland, Collins, Stevens, Helms
was scheduled for Senate vote

As substantially revised, attempts to strengthen federal information security practices and coordinate government information security efforts with those of the civilian, security, and law enforcement communities.

S. 2092 — (no short title)
Schumer, Kyl
referred to Judiciary Committee

Would ease law-enforcement monitoring of electronic communications, modify fraud and related computer-crime provisions, etc.

S. 2430 — Internet Security Act of 2000
Leahy
referred to Judiciary Committee

Would greatly broaden federal jurisdiction over computer hacking cases, permit forfeiture of property used in computer hacking crimes, increase the availability of law-enforcement wiretapping, and eliminate mandatory minimum sentences for certain computer hacking crimes.

S. 2448 — Internet Integrity and Critical Infrastructure Protection Act of 2000
original version: Hatch, Schumer, Abraham, Kyl
current version: Hatch, Leahy, Schumer
was scheduled for Senate vote

Originally, this was a very large piece of legislation. Some of the highlights were: enhanced penalties for computer crimes, civil and criminal forfeiture of property used in such crimes, increased coordination between the FBI and the Secret Service, increased availability of law-enforcement wiretapping, penalized "commercial disparagement" using the Internet, curbed unsolicited email, increased privacy protection for personal information, and increased funding for the National Infrastructure Protection Center.

The version that is scheduled for a vote by the Senate was completely rewritten, dramatically reducing its scope, and harmonizing it somewhat with S. 2430 (above). As amended, S. 2448 would, among other things, give the Secret Service jurisdiction to investigate certain computer crimes, including those against financial institutions, increase penalties for criminal activity that used encryption; authorize $5 million to establish a Deputy Assistant Attorney General to oversee DoJ's Computer Crime and Intellectual Property Section, and give DoJ $80 million to create 10 regional computer forensic labs that would provide education, training, and forensic capabilities to state and local law enforcement charged with investigating computer crimes, and another $20 million to establish a National Cyber Crime Technical Support Center. The bill would also permit the confiscation of equipment used to commit computer crimes, allow the prosecution of juveniles, increase various computer-crime penalties to as much as 20 years in

prison, and would require the U.S. Sentencing Commission to review and perhaps revise the sentencing guidelines for computer crimes, including elimination of the six-month mandatory minimum sentence for reckless crimes.

Dropped from the bill is removal of the requirement that $5000 in damage is necessary for federalizing computer crime (jurisdiction established by definition of "damage" in Computer Fraud & Abuse Act, 18 U.S.C. § 1030), and any provision for law enforcement to obtain a single, nationwide "trap and trace" court order intended to make it easier to track computer criminals operating or committing crimes across several states or time zones. Because it is vastly different from the House-passed cybercrime bill (H.R. 5018, above), no further action is likely at this late date in the legislative year.

S. 2451 — (no short title)
Hutchison
referred to Judiciary Committee

Would create a National Commission on Cybersecurity, and increase penalties for, and broaden the applicability of, computer crimes.

S. 3188 — Cyber Security Enhancement Act
Kyl, Feinstein
referred to Judiciary Committee (introduced October 11)

S. 3188 would call for more protection for U.S. critical infrastructure from hackers, terrorists, and rogue nations by allowing entities to voluntarily submit information that the government would not otherwise have about weaknesses in their online systems, as well as information on threats and attacks to the federal government, without fearing that the information would be subject to disclosure under the Freedom of Information Act. In addition, S. 3188 would permit the Attorney General to issue administrative subpoenas to trace cyberattacks, and would require the A.G. to report to Congress on plans to standardize information requests to business, and efforts to encourage the technological prevention of falsifying e-mail addresses.

Military

Department of Defense

The Pentagon's Joint Task Force for Computer Network Defense is completing a common database to enable the defense and intelligence communities in DoD, the intelligence agencies, and the FBI to share information critical to protecting their networks against intruders, and is to be operational in early 2001.

Defense Advanced Research Projects Agency

DARPA has awarded four contracts to Secure Computing Corp., adding more than $6 million to research and development for secure networks. Three of the contracts

are for programs within DARPA's Third Generation Security Initiative, aimed at developing advanced mechanisms to secure DoD's critical infrastructure systems against cyberattack.

U.S. Space Command

Spacecom is considering whether to form a unified subcommand to take charge of computer network defense and attack missions. Spacecom has been responsible for computer network defense missions and recently added the computer network attack responsibilities, including offensive information operations such as cyberattacks against enemy networks that control air defense systems. Spacecom is now studying the best organization for conducting the two types of missions, including separate task forces for the two missions, one joint task force for both, or a subcommand for both.

International

Department of Commerce International Trade Administration (and others)

In October, a delegation of U.S. e-commerce trade officials from the White House and several agencies met with their European counterparts to discuss issues of mutual concern, including infrastructure and information security. They hope to establish an "early warning system" for regulatory differences to prevent future conflicts similar to those that occurred over privacy.

Council of Europe, "Draft Convention on Cyber-crime"

open for public comment (email: *DAJ@COE.INT*)

Since September 2000, the Council of Europe released revisions of its Draft Convention on Cyber-crime, which would grant police much greater powers to access electronic information. The convention is an attempt to standardize computer crime statutes throughout Europe, and require signatories to cooperate with one another. The Council of Europe was pushing for an agreement on the Convention by December. If approved in Europe, the treaty could be additional impetus to create stricter cybercrime legislation within the U.S.

The convention proposes, among other things, that countries adopt laws criminalizing unauthorized computer access or data interception or manipulation, as well as the possession of passwords or other common security tools if they are held with the intent to commit an offense. It also proposes laws to enable government access to encrypted information and to expand copyright protections.

However, a coalition of 28 prominent international cyber-rights organizations have come out against the current draft, stating that it could result in outlawing network security tools and would require entities to review and keep extensive logs of the message traffic on their systems. In a letter sent to the Council of Europe Secretary General, the Global Internet Liberty Campaign, which includes prominent groups from the U.S., France, Britain, Australia, Bulgaria, Canada, Italy, South Africa,

Austria, the Netherlands, and Denmark, claims the treaty is little more than a law enforcement wish list. A U.S. DoJ official has also stated that the U.S. government is not in favor of the data-retention requirement, and would prefer self-regulation and less intrusion on business.

ATTACHMENT L: REPORTED CYBER AND OTHER INCIDENTS

Cyber Incidents

Recent Insider Cyber incidents include the following:

- January 2001 – John Deutch, former Director of the CIA is pardoned. Deutch downloaded highly classified information on his home computer while he was Director of the agency. Many individuals, including a foreign national employed in his home, had access to this computer.
- October 2000 – An engineer who left Cisco systems in October of 2000 and went to work for a competitor, Calix Networks, was charged with stealing trade secrets. He is reported to have copied many computer files, e-mails, etc., before leaving Cisco. If found guilty, he could be sentenced to 10 years and fined $250,000.
- May 2000 – Timothy Lloyd was convicted of causing $12 million in damages to Omega Engineering, his former employer. He had planted a logic bomb that destroyed contracts and software.
- March 2000 – Abdelkader Smires, a programmer at ITTI, tried to extort greater pay and benefits from his employer. When his demands were refused, he was caught in the act of attacking the company's computer systems.
- September 1999 – In January 2001, the British Government acknowledged that, in September 1999, a security guard at the Bradwell Nuclear Plant attempted to hack into the plant computer system.
- 1999 – Shakuntla Devi Singla, a civilian employee of the U.S. Coast Guard, uses another employee's password to delete a personnel database. It takes 115 employees over 1800 hours to reconstruct the information.

Workplace Liability and Employee Safety

At least four companies have been successfully sued or are being sued for failing to properly screen applicants who turned violent on the job.

- In 1998, a jury awarded $7.9 million to the families of two North Carolina men killed by a co-worker in a warehouse operated by Union Butterfield and Dormer Tools.
- Two Atlanta Trading firms, Momentum Securities and All-Tech Investment Group, are fighting at least ten lawsuits filed after the 1999 workplace shootings by former day trader Mark Barton (nine killed and four wounded).
- Xerox Corp. is facing at least one suit in the 1999 Hawaiian office shootings by copy machine repairman Byran Uyesugi.